(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
31 January 2002 (31.01.2002)

PCT

(10) International Publication Number
WO 02/09387 A1

(51) International Patent Classification[7]: H04L 29/06, 29/12

(21) International Application Number: PCT/EP00/07037

(22) International Filing Date: 21 July 2000 (21.07.2000)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicants *(for all designated States except US)*: **NOKIA CORPORATION** [FI/FI]; Keilalahdentie 4, FIN-02150 Espoo (FI). **BERTÉNYI, Balázs** [HU/HU]; Nagyszalonta u. 6, H-1118 Budapest (HU).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **BAJKÓ, Gábor** [HU/HU]; Damjanich u. 26/B, H-1072 Budapest (HU). **KISS, Krisztián** [HU/HU]; Bimbó u. 126, H-1026 Budapest (HU).

(74) Agents: **LESON, Thomas, Johannes, Alois** et al.; Tiedtke-Bühling-Kinne, Bavariaring 4, D-80336 Munich (DE).

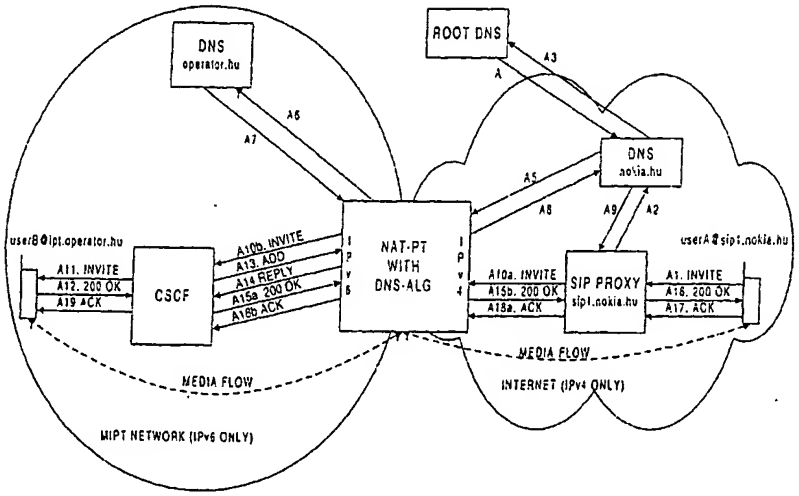
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) Title: SIP SESSIONS BETWEEN IPV4 AND IPV6 CLIENTS AND SIP BASED CALL SETUP IN 3GPP IP MULTIMEDIA SUBSYSTEM WITH NAT IN PLACE



(57) Abstract: The invention proposes a network system, comprising a first and a second network, a network control device (CSCF) located in the first network and a network address translation device (NAT or NAT-PT) located at a border between the first network and the second network; wherein the network control device and the network address translation device are adapted to exchange commands of a special control protocol, the network control device is adapted to effect address translation of addresses included in the payload of a data packet by sending (A13) a command of the special control protocol to the network address translation device, and the network address translation device is adapted to translate the address received by the command of the special control protocol and to forward (A14) a command of the special control protocol including the translated address to the network control device. The invention also proposes a corresponding method.

WO 02/09387 A1

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

"SIP sessions between IPv4 and IPv6 clients and SIP based call setup in 3GPP IP multimedia subsystem with NAT in place "

--

Field of the invention

The present invention relates to a network system and a method for traversing multimedia communication via network borders.

BACKGROUND OF THE INVENTION

The invention relates to the so-called Session Initiation Protocol (SIP). SIP is a general-purpose tool for the initiation, modification, and termination of sessions. That is, SIP is an application-layer control (signalling) protocol that can establish, modify and terminate multimedia sessions or calls with one or more participants. These sessions include Internet multimedia conferences, Internet telephone calls, multimedia distribution and similar applications. Members in a session can communicate via multicast or via a mesh of unicast relations, or a combination of these. As a core part of its functionality, SIP carries the ports, IP addresses and domain names needed to describe the sessions it controls.

SIP can be used to initiate sessions as well as to invite members to sessions that have been advertised and established by other means. Sessions can be advertised using multicast protocols such as SAP, electronic mail, news groups, web pages or directories, among others.

SIP invitations used to create sessions carry session descriptions which allow participants to agree on a set of compatible media types. SIP supports user mobility by proxying and redirecting requests to the user's current location. Users can register their current location. SIP is not tied to any particular conference control protocol. SIP is designed to be independent of the lower-layer transport protocol and can be extended with additional capabilities.

In the following, the SIP invitation is described in more detail. A successful SIP invitation consists of two requests, INVITE followed by ACK. The INVITE request asks the callee to join a particular conference or establish a two-party conversation. The callee can agree to participating in the call by sending a 200 OK response. In turn, the caller confirms that he has received that response by sending an ACK request. If the caller no longer wants to participate in the call, it sends a BYE request instead of an ACK.

Recently 3rd Generation Partnership Project (3GPP) has selected SIP as the call control protocol for 3G (3rd Generation) IP-based wireless networks.

The limited size that the current IPv4 (Internet Protocol version 4) protocol address space can offer has been causing difficulties in coping with the explosive increase of the amount of IP addresses needed. This situation will culminate with the introduction of cellular data services, such as General Packet Radio Service (GPRS) and Mobile IP Telephony (MIPT). For the new generation of applications such as Mobile IP Telephony and push applications, unique addressing and

end-to-end client reachability will be fundamental. Using IPv4 does not offer a viable solution and IPv6 (Internet Protocol version 6) must be considered to be used within cellular data services. The 3GPP standardisation organisation has recently selected IPv6 as the only network protocol for the Mobile IP Telephony Network. However, the timeframe for changing/upgrading the current IPv4 devices to IPv6 is difficult to foresee, thus the communication between the legacy IPv4 and the newly introduced IPv6 devices must be solved. The interworking is not limited to simple IP protocol translation (between v4 and v6) since there are applications which include transport addresses (TA) in the packet payload (eg. SIP, FTP) to establish new media or data connections.

This interworking between different protocols is performed by so-called Network Address and Protocol Translators (NAT-PT). A NAT-PT or NAT is a logical function which is embedded in a border router which straddles a public and a private network. The NAT translates IP address information from packets which traverse the boundary.

NATs are stateful devices. They generally require a table to be established listing the active sessions. For each session, the particular bindings and translations are stored. Sessions are either removed explicitly through packets (e.g. TCP FIN bit checked) or are timed out after a time period (the case of UDP sessions).

Since NATs operate at the IP and transport layers, they are insufficient when application layer protocols include IP addresses and ports within their payloads.

In detail, NAT-PT is an IPv4-to-IPv6 transition mechanism which attempts to provide transparent routing to end-nodes in v6 realm trying to communicate with end-nodes in v4 realm and vice versa. This is achieved using a combination of Network Address Translation and Protocol Translation. This mechanism does not mandate dual stack in end nodes and does not have any special routing requirement neither requires tunneling support. This mechanism is based on NAT-like address translation and IP header conversion.

NAT-PT uses a pool of IPv4 addresses for assignment to IPv6 nodes on a dynamic basis as sessions are initiated across IPv4-IPv6 boundaries. The IPv4 addresses are assumed to be globally unique. NAT-PT binds addresses in an IPv6 network with addresses in an IPv4 network and vice versa to provide transparent routing for the datagrams traversing between address realms. This requires no changes to end nodes and IP packet routing is completely transparent to end nodes. It does, however, require NAT-PT to track the sessions it supports and mandates that inbound and outbound datagrams pertaining to a session traverse the same NAT-PT router.

When more IPv6 hosts want to communicate through the IPv4-IPv6 boundary than the available IPv4 addresses would allow, NAT-PT must be able to translate not only the IP addresses but also the port numbers. The TCP/UDP ports of the IPv6 nodes are translated into TCP/UDP ports of the NAT-PT's IPv4 address pool. Such a device is also known as Network Address and Port Translator, Protocol Translator (NAPT-PT).

Hosts in IPv4-realm access IPv6-realm hosts by using Domain Name Server (DNS) for address resolution. A DNS

Application Level Gateway (DNS-ALG) must be employed in conjunction with NAT-PT to facilitate name to address mapping. Specifically, the DNS-ALG must be capable of translating IPv6 addresses in DNS queries and responses into their IPv4-address bindings, and vice versa, as DNS packets traverse between IPv6 and IPv4 realms.

SIP messages carry the descriptions of the media sessions to be established in their payload using the Session Description Protocol (SDP). There has been a SIP extension defined how to modify the Via header in the SIP message body after the message has traversed a NAT. This mechanism is called receiver tagging and is intended to ensure that the SIP responses are routed back correctly through NAT.

As mentioned above, control protocols for establishing media sessions like SIP cause problems for NAT-like devices, since the addresses for the sessions to be established are carried in the body of the application layer messages. The NAT function in NAT-PT (NAT) is application unaware and does not snoop the payload. Hence, some additional mechanism is needed for payload modification.

SUMMARY OF THE INVENTION

Therefore, the object underlying the invention resides in solving the above-described problem.

According to the invention, this object is solved by a network system, comprising

a first network and a second network;

a network control device located in the first network and

a network address translation device or a network address and protocol translation device located at a border between the first network and the second network; wherein

the network control device and the network address translation device (NAT or NAT-PT) are adapted to exchange commands of a special control protocol,

the network control device is adapted to effect address and possibly protocol translation of addresses included in the payload of a data packet by sending a command of the special control protocol to the network address translation device (NAT or NAT-PT), and

the network address translation device (NAT or NAT-PT) is adapted to translate the address received by the command of the special control protocol and to forward a command of the special control protocol including the translated address to the network control device.

Alternatively, the above object is solved by a network communication method for communication between a first network and a second network, wherein in the first network a network control device is located, and at the border between the first and the second network a network address translation device or network address and protocol translation device is located at a border between the first network and the second network, the network control device and the network address translating device (NAT or NAT-PT) being adapted to exchange a special control protocol; the method comprising the steps of

receiving a message including an address to be translated within the payload of the message by the network control device,

sending a command of a special control protocol from the network control device to the network address translation device,

translating the address received by the command of the special control protocol in the network address translating device, and binding these two addresses in the network translation device for the time of the multimedia session,

sending a command of the special control protocol including the translated address to the network control device.

By the above system and method it is possible to translate addresses which are included in the payload of data packets, although the network translation address is only adapted to translate the addresses of the data packets itself. That is, by providing the network address translation device with the capability of understanding a few additional commands of a special control protocol, the translation of such addresses can easily be performed by an interworking between the network control device and the network translation device.

In particular, the control protocol should comprise a command, into which the network control device can include an address to be translated and by which the network address translation device can easily extract the address. Thus, the network address translating device can easily translate the address without actually working on the application layer.

Thus, the first and the second network can be operated with different versions of the IP network layer protocol, and/or a different addressing scheme is used in the first and the second network. The different addressing scheme

could reside in a scenario in which the first network uses a private addressing scheme and the second network uses a public addressing scheme, for example. Thus, according to the invention a multimedia communication can easily be setup in such a scenario.

Preferably, the special control protocol is the MEGACO (H.248) protocol. In this case, the network address translating device needs only to be able to handle a small subset of the MEGACO commands. For example, the ADD, SUBTRACT, and the ServiceChange command are sufficient.

The data packets may include addresses within their payloads which are part of Session Initiation Protocol (SIP) messages. Thus, the addresses which are included in SIP INVITE messages, for example, can be easily translated by the above system and method.

The network control device may be a Call State Control Function (CSCF) or a proxy, like a SIP proxy in case SIP is used. Since the CSCF or proxy has to perform application layer operations anyway, it is seen advantageous to let these devices also operate with respect to the address and protocol translation. Furthermore, CSCF may use MEGACO for controling other elements, like circuit switched gateways also.

The network address translation device may be a Network Address Translator (NAT) or a Network Address Translator and Protocol Translator (NAT-PT).

The messages exchanged may be used for initiating a multimedia communication. Such messages include addresses

in their payloads which have to be translated in order to initiate such a communication.

The network address and protocol translation device may perform a dynamic binding for media addresses which are exchanged in the initiation and modification phase of the multimedia communication. This binding is only possible by performing the above translation of addresses hidden in payloads of data packets.

The network translation device may further comprise a Domain Name Server Application Layer Gateway (DNS-ALG). By these means, a DNS query can traverse the network border. Thus, name to address mapping is facilitated, and a domain query traversing the borders can easily be performed.

In particular, in the system addresses are transported in the payload of DNS messages, and these addresses have to be changed at the network borders. It is noted that the binding of these addresses may be static in the NAT-PT, since they are addresses of network elements, thus the performance is not a critical issue in this case.

Moreover, in order to minimise the conversion complexity, the SIP message headers should not contain IP-addresses as part of SIP-URLs, usage of domain names is preferred instead, since domain names do not need any conversion.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will be more readily understood with reference to the accompanying drawings in which:

Fig. 1 a network system comprising a Mobile IP Telephony network and Internet, in which a SIP invitation procedure is carried out starting from the Internet, according to a first embodiment,

Fig. 2 the network system according to Fig. 1, in which a SIP invitation procedure is carried out starting from the MIPT network,

Fig. 3 a more detailed illustration of certain procedure messages of Fig. 1,

Fig. 4 a more detailed illustration of certain procedure messages of Fig. 2,

Fig. 5A and 5B a diagram indicating information flow between network nodes for a call originated in the Internet according to a second embodiment,

Fig. 6A and 6B a diagram indicating information flow between the network nodes for a call originated in the MIPT network,

Fig. 7 a diagram illustrating two private networks connected via a public network according to a third embodiment, and

Fig. 8A to 8D a diagram indicating information flow between the network nodes according to the third embodiment shown in Fig. 7.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

In the following, the general idea of the invention is described.

As mentioned above, NAT-PTs (NATs) operate at the IP (Internet Protocol) and transport layers, and thus they are insufficient when application layer protocols include IP addresses and ports within their payloads.

One solution for allowing SIP through NAT-PTs or NAT is using an Application Level Gateway (ALG) which understands SIP on top of NAT-PT (SIP-ALG). These devices have awareness of the particular application, and can translate addresses within message bodies.

Since in this case the proxy and NAT-PT (NAT) are collocated, the proxy can have direct control over the NAT-PT through some kind of internal API (Application Programming Interface). This configuration is advantageous in a sense that it does not need to rely on the existence of SIP servers within the network.

However, the disadvantage of this method is that the NAT-PT (NAT) would not be able to work at the desired speed since an ALG is on top of it. This may result in low performance and, even more, in dropped calls. Furthermore, the NAT-PT (NAT) needs to be upgraded each time new extensions to SIP get deployed. This eventually may become difficult to manage and difficult to support within a wide area network.

Thus, according to the invention, the proxy and NAT-PT (NAT) are separated devices. Therefore, an external control protocol or API (Application Programming

Interface) must be used between them. This protocol would allow the proxy to instruct the NAT-PT to create or delete bindings for the media streams. This allows application layer information to be externalised from the NAT-PT.

For remotely controlling the NAT-PT (NAT), according to the invention the MEGACO (H.248) protocol is used as control protocol between the CSCF and NAT-PT.

The MEGACO protocol is a protocol used between elements of a physically decomposed multimedia gateway.

In the following some terms of the MEGACO protocol which are important for the present invention are described in short.

It is noted that a Context, as understood in the MEGACO protocol, is an association between a number of Terminations. The Context describes the topology (who hears/sees whom) and the media mixing and/or switching parameters if more than two Terminations are involved in the association. On the other hand, a Termination, as understood in the MEGACO protocol, is a logical entity on a MG (Media Gateway) that sources and/or sinks media and/or control streams. A Termination is described by a number of characterizing properties, which are grouped in a set of Descriptors that are included in commands. Terminations have unique identities (TerminationIDs), assigned at the time of their creation.

Descriptors are the parameters to a command. A Descriptor consists of a name and a list of items. Some items may have values. Next, some Descriptors and their use are described.

The Descriptor 'Stream' describes a list of Remote/Local/LocalControl descriptors for a single stream.

The Descriptor 'Local' contains properties that specify the media flows that the MG receives from the remote entity.

The Descriptor 'Remote' contains properties that specify the media flows that the MG sends to the remote entity.

In the present invention, basically three MEGACO commands are concerned, the ADD command, the SUBSTRACT command and the ServiceChange command. The ADD command adds a termination to a context and can be used to reserve resources. The ServiceChangecommand registers controlled elements to their controllers.. The SUBTRACT command disconnects a Termination from its Context and returns statistics on the Termination's participation in the Context. Thus, it can be used to release resources.

When a Termination is added to a Context, the value of its read/write properties can be set by including the appropriate descriptors as parameters to the ADD command. Properties not mentioned in the command retain their prior values.

According to the present invention, MEGACO is used for reserving and binding the TAs of the initiated media stream.

Now, the fields in the SIP/SDP (Session Description Protocol) message which contain logical names or IP addresses/port numbers are described.

In the following, the relevant SIP header fields are described:

- The Contact Header in SIP requests and responses. The Contact Header contains a SIP URL (Uniform Resource Locator). SIP URLs can contain an IP address or a hostname.

- The Record-Route and Route headers in SIP requests. They indicate routing instructions for subsequent messaging.

- The Request URI (Uniform Resource Identifier) in SIP requests. This field contains a SIP URL. It usually does not contain an IP address but a domain name.

- The Via Headers in SIP requests. They contain IP addresses or domain names and port numbers. These addresses are used to forward responses. SIP supports receiver tagged via fields. This means that if a request arrives from a host, and the source IP address in the packet containing the request does not match the address in the Via field, the proxy tags the Via field with the source IP address. This address is used to send responses. This feature means that the Via field does not need to be translated through NAT-PTs (NATs). Responses are sent to the port in the Via field and not to the source port of the message. This means that changes to the port numbers, made by NAT-PTs, will cause responses to be misrouted.

- Call-ID in a SIP request. This field contains some identifier appended to the IP address or hostname of the machine where the call was originated. This address is

never needed for message routing but it is required to be globally unique. Two users from two different private networks with same private IP addresses should never use the same identifier.

- To and From fields in SIP requests. Theses fields contain SIP URLs. Since these fields are used for identification of the parties, they should contain domain names and not IP addresses.

The following fields in the SDP part are concerned:

- The "o field". This field contains the user's host name.

- The "c field" and the "m field". These fields specify the address and port number, respectively, the user awaits for media connection. If the message passes through a NAT-PT (NAT), a new mapping with this address and port must be inserted into the NAT-PT table.

Thus, when a SIP control connection is to be set up through a NAT-PT, the following action must be taken:

The NAT-PT must be instructed to insert a mapping containing the transport addresses of the parties for media connection found in SDP's c and m fields. The media connection can comprise a RTP (Real Time Transport Protocol) connection, for example.

The NAT-PT must not translate the port number in the received SIP INVITE message when it translates the IP address. Otherwise the 200 OK response to the INVITE message will be misrouted by the SIP proxy (see Via headers above).

In the following, preferred embodiments of the invention are described in more detail with reference to the accompanying drawings.

Fig. 1 illustrates a network system comprising an Mobile IP Telephony (MIPT) network which is connected to the Internet according to a first embodiment. The MIPT network uses the IPv6 protocol, whereas the Internet uses the IPv4 protocol. Hereinafter, setting up an end-to-end SIP-session between an end-user residing in the MIPT-network and a SIP-client on the Internet is described.

The scenario is analyzed from three different perspectives: Domain name resolution, SIP-packets traversing the NAT-PT, and required SDP-payload modifications, and the usage of MEGACO to remotely control the bindings in NAT-PT.

Fig. 1 describes the detailed scenario for a call initiated by a SIP-client residing in the v4-only Internet as a first embodiment.

For performing interworking between the two different networks, the NAT-PT is applied. As illustrated, the NAT-PT comprises a DNS-ALG, i.e., a Domain Name System Application Layer Gateway. IPv4 name-to-address mappings are held in the DNS with so-called "A"-records. On the other hand, IPv6 name-to-address mappings are at the moment held in the DNS with so-called "AAAA" records. A SIP-client on the Internet may be bound to a SIP server in a sense that the domain part of its alias equals to the fully qualified domain name of its SIP server. In a MIPT network the fundamental concept of mobility assumes that the subscriber address of the mobile user does not

reflect the domain name of the CSCF (Call State Control Function) it is currently registered to.

Next, the domain name resolution in a call from the Internet (the IPv4 network) to the MIPT network (IPv6 network) is described.

In the present embodiment, a case is assumed in which an IPv4 network user (user A) wants to contact a user from an IPv6 network (user B). Thus, user A (having the address userA@sip1.nokia.hu, for example) sends a SIP INVITE message A1, which is received by a SIP proxy (having the address sip1.nokia.hu). The user B to be contacted has the address userB@ipt.operator.hu, for example.

Before the message can traverse the NAT-PT, a DNS query message must be performed, since the addresses found in the IP header and in the payload have to be translated, with the help of a DNS-ALG. The DNS name resolution process is shown in Fig. 1 with message numbers A2-A9.

In detail, in message A2 the SIP proxy sends a name resolution request (type A) asking the IP address for ipt.operator.hu to a DNS having the address nokia.hu, which is the DNS of the SIP proxy.

In message A3 the SIP Proxy's DNS forwards the request to its Root DNS.

In message A4 the Root DNS answers with the address of (type A record) MIPT network operator's DNS server. It is noted that this needs a correct configuration in the DNS system. Since the communication is in the IPv4 network, the Root DNS must be configured with an IPv4 address from

NAT-PT's address pool pointing to the MIPT network operator's DNS server (operator.hu).

Furthermore, in message A5 the SIP Proxy's DNS server contacts the DNS server of operator.hu and asks for the ipt.operator.hu IP address. NAT-PT recognizes a DNS packet based on the fact that its source and/or destination port number is 53 (either UDP or TCP).

In message A6 the DNS-ALG of the NAT-PT modifies the Query type from A to AAAA. The NAT-PT changes the destination address to the address of the operator's internal DNS and translates the source address from IP4 to "IP4 translated IP6 address".

In message A7 the operator's internal DNS sends the response message (type AAAA) back to the "IP4 translated IP6" destination address. It is noted that the routers inside the operator's backbone need a static route configuration: all packets with the destination address of type "IP4 translated IP6" must be routed to the NAT-PT.

In message A8 the DNS-ALG intercepts the packet and modifies the record type from AAAA back to A. It replaces the IPv6 address resolved by the operator's internal DNS with an IPv4 address from its address pool. It will hold the mapping between these two addresses (temporary binding). It is noted that in a flat MIPT network no such binding is needed, since NAT-PT can be configured to route all IP packets coming from the IPv4 network to port 5060 (SIP messages) to the CSCF(s). NAT-PT changes back the "IP4 translated IP6 address" destination address to IP4 and puts its address in the source field. It sends the packet to the SIP proxy's DNS.

In message A9 the DNS forwards the DNS Response to SIP proxy.

In the scenario above it is assumed that the DNS system works in the way it works today. That is, DNS has recursive mode enabled only for queries coming from local hosts.

Next, the domain name resolution in a call from the MIPT network to the Internet is described by referring to Fig. 2. Similar to the case of Fig. 1, the procedure is started by sending a SIP INVITE message in message B1, this time by user B.

An issue here is how the IPv6 only operator.hu DNS server talks to the IPv4 only (Root) DNS server outside the IPv6 domain. The external Root DNS server needs to point to an IPv4 address, part of the IPv4 pool of addresses available to the NAT-PT. The NAT-PT keeps a one-to-one mapping between this IPv4 address and the IPv6 address of the internal operator.hu IPv6 DNS server. In the other direction, the IPv6 DNS server points to a v6 address formed from the IPv4 address of the external IPv4 DNS and the prefix in use by the IPv6 domain (prefix::/96).

In order to minimize the IPv6 to/from IPv4 translations, a DNS server function is proposed in NAT-PT. If this DNS server has the recursive mode enabled in the IPv6 domain, no protocol translations are needed during the name resolution process. The scenario is described in Fig. 2 by messages B2-B11.

These message are basically similar to messages A2-A9 of Fig. 1, thus, only short description is given here. In

message B2, the CSCF sends a DNS query to its DNS (i.e., operator.hu). The DNS forwards this query to the NAT-PT in message B3. The NAT-PT sends the query to its Root DNS in message B4 which replies in message B5. Since also the Root DNS does not know the domain name, the NAT-PT forwards the query to the basic DNS having the domain .hu in message B6, which replies in message B7 giving the address of the DNS nokia.hu. Thereafter, the NAT-PT forwards the query to the DNS nokia.hu in message B8 which replies with message B9. The NAT-PT forwards this message including the address of the SIP proxy to the MIPT operator's DNS in message B10, which forwards it to the CSCF in message B11.

Protocol translation is only done when forwarding message B3 to the Root DNS and when message B9 (the DNS Response) is forwarded to the operator's DNS.

Next it is described how the SIP messages (in particular, the INVITE message) and their SDP-payload traverse the NAT-PT.

SIP carries the session description in its payload using SDP. Here it is assumed that the calling party always puts its complete SDP proposal into the INVITE message, and the called party answers with the accepted SDP in the 200 OK message.

First, a call from the IPv4 network (Internet) to the MIPT v6 network is described. The message numbering in Fig. 1 is used when describing the messages in the subsections below.

In the following, the source and destination IP-addresses of packets carrying the SIP messages are listed.

INVITE

[SIP Proxy to NAT-PT]: dest. IP addr.=$IP4_{NAT-PT}$:5060
(Message A10a) source IP addr.=$IP4_{SIP\ PROXY}$:XX

[NAT-PT to CSCF]: destination IP addr.=$IP6_{CSCF}$:5060
(Message A10b) source IP addr.=($IP4_{SIP\ PROXY}$:XX)
translatedIP6 (port# unchanged)

200 OK

[CSCF to NAT-PT]: destination IP addr.=($IP4_{SIP\ PROXY}$:XX)
translatedIP6
(Message A15a) source IP addr.= $IP6_{CSCF}$:5060

[NAT-PT to SIP Proxy]: dest. IP addr.=$IP4_{SIP\ PROXY}$:XX
(Message A15b) source IP addr.=$IP4_{NAT-PT}$:5060

ACK

[SIP Proxy to NAT-PT]: dest. IP addr.= $IP4_{NAT-PT}$:5060
(Message A18a) source IP addr.=$IP4_{SIP\ PROXY}$:XX

[NAT-PT to CSCF]: destination IP addr.=$IP6_{CSCF}$:5060
(Message A18b) source IP addr.=($IP4_{SIP\ PROXY}$:XX)
translatedIP6 (port# unchanged)

xx is an arbitrary TCP or UDP port number. It is noted, that for the exchange of the above messages no binding is necessary.

In the following, the IP-addresses carried in the SDP-payload are described. The INVITE and 200 OK messages carry the following addresses for media in the SDP part:

INVITE

[SIP Proxy to CSCF]: $IP4_{media}$ advertised in SDP
(Messages A10a and A10b)

[CSCF to IP6 terminal]: $IP4_{media}$ translated IPv6
(Message A11)

200 OK

[IP6 terminal to CSCF]: $IP6_{media}$ advertised in SDP
(Message A12)

[CSCF to SIP Proxy]: $IP4_{NAT-PT}$ copied from MEGACO REPLY
(Message A12)

'IP4 translated IP6' is an address of the form PREFIX::ffff:0:IP4, where PREFIX is an identifier assigned to the IP6 network.

It is assumed that both the SIP Proxy and CSCF are stateful devices, that is, in case of an ongoing call setup they can tie a certain SIP message to the correct call state machine (i.e., CSCF or SIP proxy) based on the call_ID header of the message.

The MIPT network needs a configuration that allows the routers to route all packets with a destination address of PREFIX::/96 to the NAT-PT.

Next, the other case, i.e., the call from the MIPT network to the Internet is described. The message numbering in Fig. 2 is used when describing the messages in the subsections below.

The following source and destination IP-addresses of packets carrying the SIP messages are described:

INVITE

[CSCF to NAT-PT]: (Message B14a)	destination IP addr.=($IP4_{Proxy}$:5060) translated IP6 (address obtained by name resolution and modified by DNS-ALG) source IP addr.=$IP6_{CSCF}$:yy
[NAT-PT to SIP Proxy]: (Message B14b)	destination IP addr.=$IP4_{Proxy}$:5060 source IP addr.=$IP4_{NAT-PT}$:yy (port# unchanged)

200 OK

[SIP Proxy to NAT-PT]: (Message B17a)	destination IP addr.=$IP4_{NAT-PT}$:yy source IP addr.= $IP4_{Proxy}$:5060
[NAT-PT to CSCF]: (Message B17b)	destination IP addr.=$IP6_{CSCF}$:yy source IP addr.=($IP4_{Proxy}$:5060) translated IP6

ACK

[CSCF to NAT-PT]: (Message B20a)	dest. IP addr.=($IP4_{Proxy}$:5060) translated IP6 source IP addr.= $IP6_{CSCF}$:yy
[NAT-PT to SIP Proxy]: (Message B20b)	destination IP addr.=$IP4_{Proxy}$:5060 source IP addr.=$IP4_{NAT-PT}$:yy (port# unchanged)

The INVITE and 200 OK messages carry the following addresses for media in the SDP part:

INVITE

[IP6 terminal to CSCF]: (Message B1)	$IP6_{media}$ advertised in SDP

[CSCF to SIP Proxy]: $IP4_{NAT-PT}$ copied from MEGACO REPLY (Messages B14a and B14b)

200 OK

[SIP Proxy to CSCF]: $IP4_{media}$ advertised in SDP (Messages 17a and 17b)

[CSCF to IP6 terminal]: $IP4_{media}$ translated IPv6 (Message B18)

According to the invention, the MEGACO (H.248) protocol is used for the CSCF to externally control the NAT-PT, which is described in the following with reference to Figs. 3 and 4.

This requires MEGACO to be implemented in the NAT-PT. However, a very basic implementation should be sufficient, since only a very small subset of MEGACO protocol's capabilities will be used. This subset is presented below.

It is noted that in the following detailed message listings additional comments are marked by '//'.

Firstly, a registration procedure is described by which the NAT-PT registers for MEGACO control with the CSCF.

The NAT-PT shall be able to register with the CSCF for MEGACO-control. This registration is conducted by means of sending a ServiceChange command, and the CSCF may accept the registration attempt with a ServiceChangeAck reply. It is noted that these registration procedure is not illustrated in the figures.

The NAT-PT sends the following message to CSCF in order to register:

```
MEGACO/1 [AB.CD.EF::12.34.99] //IPv6 address of NAT-PT
 Transaction = 9999 {
    Context = - {
       ServiceChange = ROOT {Services {
          Method=Restart,
          ServiceChangeAddress=55555, Profile=ResNAT/1}
       }
    }
 }
```

CSCF sends a reply to NAT-PT accepting the registration:

```
MEGACO/1 [AB.CD.EF::12.34.56]:55555  //IPv6 addr. of CSCF
Reply = 9999 {
   Context = - {ServiceChange = ROOT {
     Services {ServiceChangeAddress=55555, Profile=ResNAT/1}}}
}
```

Next, it is described how the CSCF controls the address-binding in NAT-PT with MEGACO.

The NAT-PT realizes only ephemeral type of terminations, this also means that the TerminationID and the local transport address in the NAT-PT to be used for the session are allocated by the NAT-PT itself, and returned to the controlling CSCF in the reply message. The CSCF initiates the binding request in NAT-PT by sending an ADD command, and receives a TA from NAT-PT to be used for the session in the reply message.

With reference to Fig. 3, a call from the Internet to the MIPT network is described. Fig. 3 shows the scenario as

described in Fig. 1 from MEGACO point of view. Thus, the message numbering in Fig. 1 is used when describing the MEGACO messages below in detail.

It is noted that the media-IP-address or media TA (Transport Address) of user B is 12.34.01:1111. In message A12, user A sends a SIP 2000 OK message. The SDP part thereof includes in field c the media-IP-address, i.e., AB.CD.EF::12.34.01. Field m includes the media port, which is 1111 in this example.

In Message A13, a MEGACO ADD message is sent from the CSCF to the NAT-PT. Thus, as mentioned above, a termination is added to the context.

```
Message A13:
MEGACO/1 [AB.CD.EF::12.34.56]:55555     //IPv6 address of
                                          CSCF
Transaction = 50001 {
    Context = $ {
        Add = $ { Media {
            Stream = 1 {
                LocalControl {Mode = SendReceive} }},
            },
            Local {
v=0
c=IN IP4 $
m=audio $ RTP/AVP 4
a=ptime:30
            },
            Remote {
v=0
c=IN IP6 media-IP-address of UserB  //The media IP-
                                      address and media-
                                      port of UserB is
                                      copied from the SDP
                                      part of the 200 OK.
m=audio media-port RTP/AVP 4        //RTP profile for
                                      G.723 is 4
a=ptime:30
            }
        }
    }
}
```

Thus, the c and m fields which has been send by the SIP 200 OK message A12 are copied in the c and m fields in the MEGACO ADD message A13.

After receiving message A12, the NAT-PT selects an address from its address pool to be bound to the address received in message A12.

In message A14, the NAT-PT replies to the CSCF by sending a MEGACO REPLY message. Therein, the 'IP4 translated IP6' obtained by the NAT-PT is included in field c. This new media IP-address is in this example 111.111.111.1.

Message A14:

```
MEGACO/1 [AB.CD.EF::12.34.99]:55555 //IPv6-address of
                                              NAT-PT
Reply = 50001 {
    Context = 5000 {
        Add = 00001{
            Media {
                Stream = 1 {
                    Local {
v=0
c=IN IP4 111.111.111.1      //CSCF puts this media IP-
                              address and port into the
                              SDP part of the 200 OK.
m=audio 1111 RTP/AVP 4 }
                }
            }
        }
    }
}
```

Thereafter, the SIP 200 OK message is forwarded from the CCSCF to the NAT-PT in message A15a. This SIP 200 OK message now includes in field c the media-IP-address as required for user A. As shown in Fig. 1, the SIP 200 OK message is forwarded from the NAT-PT to the SIP proxy in

message A15b, and the SIP 200 OK message is forwarded in message A16 from the SIP proxy to user A.

User A acknowledges the 200 OK message by sending an ACK in message A17. This message is first sent to the SIP proxy, which forwards it to the NAT-PT. Here, the address is translated and thereafter, the ACK is forwarded to the CSCF in message A18b. Finally, the CSCF forwards the ACK to user B in message A19. Thereafter, the media flow can be started.

In the following, with respect to Fig. 4 the scenario of Fig. 2 is described from MEGACO point of view in detail, wherein the message numbering in Fig. 2 is used.

As described above in conjunction with Fig. 2, in message B1 the user A sends a SIP INVITE message in order to initiate a media session with user A. The SIP INVITE message is sent to the CSCF. In particular, in the SDP part thereof, the media IP-address and port are included, similar as in Fig. 3.

In message B12, a MEGACO ADD message is sent to the NAT-PT.

```
Message B12:
MEGACO/1 [AB.CD.EF::12.34.56]:55555
Transaction = 50001 {
   Context = $ {
      Add = $ { Media {
           Stream = 1 {
              LocalControl {Mode = SendReceive} }},
           },
           Local {
v=0
c=IN IP4 $
m=audio $ RTP/AVP 4
a=ptime:30
           },
           Remote {
v=0
c=IN IP4 media-IP-address of UserA  //The media IP-
                                      address and media-
                                      port of UserA is
                                      received in the
                                      SDP part of the
                                      INVITE.
m=audio media-port RTP/AVP 4
a=ptime:30
                }
             }
          }
       }
   }
}
```

In message B13, the NAT-PT replies to the CSCF with a MEGACO REPLY message. In this message the "IP4 for IP6 address" is included in field c, similar to the example of Fig. 3.

```
Message B13:
MEGACO/1 [AB.CD.EF::12.34.99]:55555
Reply = 50001 {
    Context = 5000 {
        Add = 00001{
            Media {
                Stream = 1 {
                    Local {
v=0
c=IN IP4 111.111.111.1          //CSCF copies this media
                                  IP-address and port into
                                  the SDP part of the
                                  INVITE.
m=audio 1111 RTP/AVP 4
}
                }
            }
        }
    }
}
```

By the above-described embodiment, SIP messages and the media sessions it initiates can be managed to get through a NAT-PT. A DNS ALG function is needed and a DNS server function with recursive mode enabled is recommended in NAT-PT.

For remotely controlling the dynamic address bindings in NAT-PT, a CSCF using MEGACO is used, as mentioned above.

Thus, the CSCF must be able to handle both type of IP addresses (IP4 or IP6) an SDP message may contain. It must be able to translate an IP4 address to an 'IP4 translated IP6' when needed. When updating the Via-

header, the CSCFs must use their domain name and not IP addresses. CSCFs should tag SIP messages (the VIA header) when messages arrive from NAT-PT and contain IP addresses instead of domain names (receiver tagging). A simple subset of the controller side MEGACO has to be implemented as described in conjunction with Figs. 3 and 4.

For the NAT-PT, a simple subset of the gateway side of MEGACO has to be implemented as described in conjunction with Figs. 3 and 4. Furthermore, a DNS-ALG has to be implemented.

As a second embodiment, a SIP scenario for an example of a Mobile Terminated (MT) call from the Internet is described.

According to the second embodiment, it is assumed that a first user located in the Internet requests a call to a second user located in a private network. The information flow between the network nodes concerned is illustrated in Fig. 5A and 5B. It is noted that Fig. 5B is a continuation of Fig. 5A.

As already described above with respect to the first embodiment, the name space and DNS records must be configured so that all incoming requests for users within the private network arrive at the NAT. If the company is named ipt1.mipt.hu, this implies that the SIP URLs published externally for users of ipt1.mipt.hu should be of the form sip:user@ipt1.mipt.hu. DNS records must be configured so that a lookup of ipt1.mipt.hu results in the address of the NAT (or NATs, when there are more than one to support load balancing).

An INVITE message arrives at the NAT (intended for the proxy) when a call is to be set up to a user inside the network. The NAT does only have to rewrite the destination IP address of the packet to the private address of the proxy (I-CSCF, i.e., the Interrogating Call State Control Function).

Address bindings are not created for the media streams in the NAT at this time. A NAT will not need to modify any of the fields of the message. The request is forwarded to the proxy (I-CSCF). All of the SIP level details regarding NAT processing are done in the proxy (I-CSCF).

That is, the VIA header is tagged with the TA address of NAT. Furthermore, the Record Route field is updated. The c and m fields in the SDP part of the INVITE message are rewritten to a TA from the private address space (this must be asked from the NAT). The proxy (i.e., the I-CSCF) records the original (c, m) fields and the changed (c', m') fields.

The message is forwarded either to the user (if I-CSCF is the S-CSCF for that MIPT user) or to the next proxy (S-CSCF) which forwards it to the user.

When a 200 OK response arrives back to the proxy (I-CSCF) from inside (based on the via headers), the proxy examines the SDP and notes the IP address and port the inside user awaits the media session on. It asks for a globally routable TA from the NAT and rewrites the SDP fields according to the received information. The OK is then forwarded to NAT.

When the ACK arrives for the 200 OK, it will pass through the NAT, and arrive at the proxy. The proxy identifies

the call based on the call_ID and request the address bindings from the NAT for the media session. The ACK is then forwarded further.

In the following, the above procedures are described in more detail with reference to the information flow diagram shown in Fig. 5A and 5B. In this scenario it is assumed that the Via and Route fields contain IP addresses instead of domain names, so no DNS queries are needed inside the private network. Furthermore, it is noted that no security issues are considered.

In the illustrated example, a first user, e.g., a user Kati located in the Internet wishes to establish a multimedia call with a user Jani located in a private network who has the domain name ipt1.mipt.hu, as described above.

In message C1, the user Kati sends a SIP INVITE message. This message is forwarded to the corresponding SIP proxy. The SIP proxy has to find out the IP address of ipt1.mipt.hu. This is effected by sending a DNS query to a DNS in message C2. The DNS responds in message C3 by sending the IP address, which is in this example 110.1.1.1. This is the IP address of the NAT of the private network. Thus, the SIP proxy forwards the INVITE message to the NAT in message C4.

The NAT translates the IP address and port in the packet header for this signalling connection in order to allow SIP packets passing through the NAT. In message C5, the NAT forwards the SIP INVITE message to the default CSCF, i.e., an Interrogating CSCF (I-CSCF).

The I-CSCF updates the VIA Header using receiver tagging. That is, the I-CSCF tags the Via filed with the source IP address of the I-CSCF.

In message C6, the I-CSCF asks the HSS for the S-CSCF of Jani. The HSS returns the S-CSCF of Jani in message C7 to the I-CSCF. By using this information, the I-CSCF forwards the SIP INVITE message to the S-CSCF in message C8. The S-CSCF, in turn, forwards the SIP INVITE message to the user Jani.

In case the user agrees to the media session to be initiated, he sends a SIP OK message (i.e., SIP 2000 OK). This message is sent to the S-CSCF in message C10 and forwarded to the I-CSCF in message C11.

The I-CSCF sends a MEGACO ADD command to the NAT in message C12. Similar as in the first embodiment, a public TA (Transport Address) is obtained, which is sent from the NAT to the I-CSCF in a reply message. After receiving the public TA, the I-CSCF overwe4rites the media address in the SDP part with the public TA. Thereafter, the SIP OK message is forwarded to the NAT in message C13.

In the NAT, the SIP OK message traverses from the MIPT network to the public Internet and is forwarded to the SIP proxy in message C14. The SIP OK message is then forwarded to user Kati in message C15.

Kati acknowledges the OK from Jani by sending a SIP ACK message to the SIP proxy in message C20. This message is forwarded to the NAT in message C17. IN message C18, the NAT forwards the SIP ACK message to the I-CSCF.

Then, the MEGACO MODIFY command is sent to the NAT in message C19. Thereby, the NAT is instructed to bind media addresses. Thus, a dynamic binding of the addresses is achieved, which is memorised in a NAT table.

The SIP ACK message is forwarded to user entity in the MIPT network, i.e., to Jani in messages C20 and C21. Thereafter, the media stream is started in message C22. In the NAT, IP addresses and UDP port s are translated according to the bindings in the NAT table.

It is noted that according to the above-illustrated embodiment, NAT decisions and bindings are still needed when translating addresses in the header of the IP packets for the signalling messages (INVITE, OK, ACK).

Next, a MO (Mobile Originated) call to the Internet is described by referring to Figs. 6A and 6B.

When a user located in the MIPT network (i.e., Jani) makes a call, the CSCF acts as a local outbound proxy. If NAT is in use at the network boundary, the following operations are performed by the CSCF:

The INVITE message is analyzed at SIP level. The IP addresses and ports in the SDP are removed. A globally routable TA address is requested from NAT. This address is inserted into the SDP. When the OK arrives for this INVITE, CSCF notes the TA in the SDP. When ACK arrives from the user inside the MIPT network, CSCF instructs NAT for the media flow binding.

If a Contact field is inserted into the INVITE message and this field contain a different address than the FROM

field, bindings must be created for both addresses in NAT.

The call scenario is shown in Figs. 6A and 6B.

In message D1, the user Kati sends a SIP INVITE message. This message is forwarded to the CSCF of Kati, i.e., the O-CSCF. The O-CSCF has to find out the IP address of sip.hu domain. This is effected by sending a DNS query to an iDNS (i.e., the internal DNS of the MIPT network, i.e., the ipt1.mipt.hu domain) in message D2. The iDNS responds in message D3 by sending the IP address.

In message D4, the O-CSCF asks for a public TA by sending a MEGACO ADD command to the NAT. The NAT replies with the public TA address, as described above in first embodiment. Thus, the O-CSCF rewrites the media private TA address contained in the SDP part of the SIP INVITE message to the public TA address provided by the NAT. Both addresses are memorised.

Thereafter, the O-CSCF forwards the SIP INVITE message (now to sip.hu proxy) to the NAT. In turn, the NAT translates the private TA to the public TA address for this message. Both addresses are bound to each other.

The NAT forwards the SIP INVITE message to the SIP proxy in message D6 which forwards it to the user located in the Internet, i.e., Kati in message D7.

If Kati is willing to accept the invitation to the media session of Jani, Kati sends a SIP 200 OK in message D8. This message is received by the SIP proxy, which forwards the SIP 200 OK message to the NAT in message D9.

The NAT translates the public TA address to the private TA address according to the previous binding. Thereafter, the SIP 200 OK message is forwarded to the O-CSCF in message D10. The O-CSCF notices the media address contained in the SDP part of the SIP 200 OK message and forwards the message to Jani in message D11.

Jani acknowledges the 200 OK message of Kati by sending a SIP ACK in message D12. This message is received by the O-CSCF which instructs the NAT for media binding by sending a MEGACO MODIFY command in message D13.

Thereafter, the O-CSCF forwards the ACK to the NAT in message D14, which forwards this message (after performing the above-described address translation) to the SIP proxy in message D15. The SIP proxy forwards the SIP ACK to user Kati in message D16.

The flowing of the media stream can be started, as shown in message D17. The NAT translates the IP address and the UDP port according to the binding in the NAT table.

Hereinafter, a third embodiment is described in which a call between two UE (User Entities) from different MIPT networks is illustrated. The two private networks are connected via the public Internet. In this case, the two private networks reach each other by sending the messages to the other network's public address. This scenario is a combination of the previous two described in the second embodiment with reference to Figs. 5 and 6.

Fig. 7 shows the network scenario for such an end-to-end SIP call through NATs at the network borders. In this example, the first private network is referred to as network A, in which user Jani is located. This network

can have the domain sonera.fi, for example. The second private network is referred to as network B, in which user Kati is located. This network can have the domain pannon.hu, for example. At the border between network A and the public Internet, a NAT1 is located, whereas at the border between network B and the public Internet, a NAT2 is located.

Fig. 8A to 8D shows the information flow between the network nodes. The messages are indicated in Fig. 7 and in Figs. 8A to 8D by the same reference characters.

The messages E1 and E2 and E5 to E7 basically correspond to the messages D1 to D6 in Fig. 6A, thus, a detailed description thereof is omitted.

However, in this example the DNS query is extended. That is, it is assumed that the query to the DNS of the network A fails. Thus, in message E3, the DNS query is forwarded to an eDNS (external DNS) located in the public Internet. The eDNS replies in message E4 with the requested address. The DNS of the network A forwards the DNS response to the O-CSCF, similar as in message C3 of Fig. 6A.

In message E7, the SIP INVITE message is forwarded to NAT1, wherein the destination TA of IP packets is changed to the I-CSCF TA address. The NAT1 translates the private source TA address to the public TA source address for this message. The NAT1 binds the addresses. The SIP INVITE message is then forwarded to the NAT2 in message E8.

The NAT2 translates the public source TA address to the private source TA address. As NAT1 does, also NAT2 binds

the addresses. In message E9, the SIP INVITE message is forwarded to the default CSCF in the network B, i.e., the I-CSCF. The I-CSCF updates the Via Header using receiver tagging, as described above. The I-CSCF starts a location query in order to obtain the S-CSCF of user Kati. Thus, it sends message E10 to the HSS (Home Subscriber Server), which replies in message E11 with the address of the S-CSCF. The I-CSCF notices the public TA address for media. Thereafter, it forwards the SIP INVITE message to the S-CSCF in message E12, which forwards the SIP INVITE message to user Kati in message E13.

If the user is willing to accept the requested media session, he sends a SIP 200 OK in message E14. The process for forwarding this message to the NAT2 are similar to that shown in Figs. 5A and 5B with respect to messages C10 to C13. Thus, a detailed description of messages E14 to E17 is omitted here.

The NAT2 translates the private source TA address to the public source TA address and forwards the SIP 200 OK message to the NAT1 via the public Internet. The NAT1, in turn, translates the public destination TA address to the private destination TA address and forwards the SIP 200 OK message to the O-CSCF in the Network A in message E19.

The following messages E20 to E23 correspond to the messages D11 to D14. That is, the NAT1 receives the SIP ACK message from user Jani in message E23.

The NAT1 translates the private source TA address to the public source TA address and forwards the SIP ACK message based on the route header to NAT2 in message E24. The NAT2 again translates the public source TA address to the

private source TA address. Then, it forwards the SIP ACK to the I-CSCF in the network B in message E25.

In message E26, the I-CSCF sends a MEGACO MODIFY command to the NAT2, in which the NAT is instructed for media TA binding. Thereafter, the SIP ACK message is forwarded from the I-CSCF to user Kati in message E27.

Then, the media stream can be started, as shown in messages E28. When traversing the border between the network B to the public Internet, the NAT2 translates the IP address and the UDP port according to the binding in the NAT table of NAT2. On the contrary, when traversing the border between the public Internet and the network A, the NAT1 translates the IP address and the UDP port according to the binding in the NAT table of NAT1.

In the following, some examples for the SIP messages in the present embodiment are described in more detail by using the numbering of the previous signalling diagram. It is noted that comments in the listing of the messages are started with '//'.

Message E1: Jani to CSCF:

```
INVITE sip:kati@ocscf.ipt1.mipt.hu SIP/2.0
Via: SIP/2.0/UDP 10.18.66.1   //originating terminal's
                                  private TA addr.
From: Jani <sip:jani@ipt1.mipt.hu>
To: Kati <sip:kati@ipt2.mipt.hu>
ALSI: sip: 244910000020001@ipt1.mipt.hu
Call-ID: 12231131@10.18.66.1 //originating terminal's
                                  private TA addr.
Cseq: 1 INVITE
Content-Type: application/sdp
Content-Length:
```

```
v=0
o=jani 76525365 41540546 IN IP4 10.18.66.1
s=Call Invitation
c=IN IP4 10.18.66.1          //IP addr. the user awaits
                               the media
m=audio 3456 RTP/AVP 0       //RTP port the user awaits
                               the media
```

Messages E7,E8,E9: O-CSCF to I-CSCF:

```
INVITE sip:kati@ipt2.mipt.hu SIP/2.0
Via: SIP/2.0/UDP 10.123.61.2 //O-CSCF.ipt1.mipt.hu IP
                               addr.
Via: SIP/2.0/UDP 10.18.66.1
From: Jani <sip:jani@ipt1.mipt.hu>
To: Kati <sip:kati@ipt2.mipt.hu>
Call-ID: 1231131@10.18.66.1
Cseq: 1 INVITE
Content-Type: application/sdp
Content-Length:

v=0
o=jani 76525365 41540546 IN IP4 10.18.66.1
s=Call Invitation
c=IN IP4 152.12.61.2         //NAT1 public IP addr.
m=audio 2321 RTP/AVP 0       //NAT1 UDP port
```

Message E12: I-CSCF to S-CSCF

```
INVITE sip:kati@scscf.ipt2.mipt.hu SIP/2.0
Via: SIP/2.0/UDP 172.16.34.2 //ipt2's I-CSCF private
                               addr.
Via: SIP/2.0/UDP 10.123.61.2; received=199.172.136.3
                     //receiver tagging, NAT2 public addr.
Via: SIP/2.0/UDP 10.18.66.1
From: Jani <sip:jani@ipt1.mipt.hu>
```

To: Kati <sip:kati@ipt2.mipt.hu>
Call-ID: 1231131@10.18.66.1
Cseq: 1 INVITE
Content-Type: application/sdp
Content-Length: 147

v=0
o=jani 76525365 41540546 IN IP4 10.18.66.1
s=Call Invitation
c=IN IP4 152.12.61.2
m=audio 2321 RTP/AVP 0

It is noted that the messages E6 and E16 are MEGACO ADD types of messages, whereas the messages E22 and E26 are MEGACO MODIFY types of messages.

As a modification of the third embodiment, the two private networks can be connected directly via a NAT. Both networks may use the same private address space.

This is basically the same scenario as above. However, the only difference is that the NAT needs a DNS ALG (as described in the first embodiment). The DNS responses are caught by the DNS ALG and the private IP address contained in the message is rewritten to an IP address from a separate address range, which is pre-configured in the NAT.

Thus according to the above-described embodiments, a SIP proxy or a CSCF can remotely control a regular NAT-PT or NAT.

Therefore, the proxy (or CSCF) and the NAT-PT (NAT) can be separated, and a special control protocol can be used between them. This protocol allows the proxy to instruct

the NAT-PT to bind or delete holes for the media streams. This allows application layer information to be externalised from the NAT-PT.

By placing the application layer awareness in the proxy rather than in NAT-PT, the NAT-PT's performance can be optimised, and newly deployed SIP extensions would only affect SIP proxies.

The special control protocol can preferably be the MEGACO (H.248) protocol. Hence, it has been shown above how SIP can traverse network address and protocol translators (NAT-PT) and also domain name resolution (DNS) issues with protocol translation have been taken under consideration.

Thus, according to the invention SIP sessions between IPv4 and IPv6 clients and SIP based call setup in 3GPP IP multimedia subsystem with NAT in place can easily be performed.

The above description and accompanying drawings only illustrate the present invention by way of example. Thus, the embodiments of the invention may vary within the scope of the attached claims. In particular, the different embodiments can be arbitrarily combined.

Claims

1. A network system, comprising

a first and a second network;

a network control device (CSCF) located in the first network and

a network address translation device (NAT) or a network address and protocol translation device (NAT-PT) located at a border between the first network and the second network; wherein

the network control device and the network address translation device (NAT or NAT-PT) are adapted to exchange commands of a special control protocol,

the network control device is adapted to effect address and possibly protocol translation of addresses included in the payload of a data packet by sending (A13; B12) a command of the special control protocol to the network address translation device (NAT or NAT-PT), and

the network address translation device (NAT or NAT-PT) is adapted to translate the address received by the command of the special control protocol and to forward (A14; B13) a command of the special control protocol including the translated address to the network control device.

2. The network system according to claim 1, wherein the special control protocol is the MEGACO (H.248) protocol.

3. The network system according to claim 1, wherein the data packets including addresses within their payloads are part of Session Initiation Protocol (SIP) messages.

4. The network system according to claim 1, wherein the network control device is a Call State Control Function (CSCF).

5. The network system according to claim 1, wherein the network control device is a proxy.

6. The network system according to claim 1, wherein the network address translation device is a Network Address Translator (NAT).

7. The network system according to claim 1, wherein the network address and protocol translation device is a Network Address Translator and Protocol Translator (NAT-PT).

8. The network system according to claim 1, wherein the messages exchanged are used for initiating a multimedia communication.

9. The network system according to claim 8, wherein the network translation device performs a dynamic binding for media addresses which are exchanged in the initiation and modification phase of the multimedia communication.

10. The network system according to claim 1, wherein the network translation device further comprises a Domain Name System Application Layer Gateway (DNS-ALG).

11. A network communication method for communication between a first network and a second network, wherein in the first network a network control device (CSCF) is located, and at the border between the first and the second network a network address translation device or network address and protocol translation device is (NAT-

PT; NAT) located at a border between the first network and the second network, the network control device and the network address translating device (NAT or NAT-PT) being adapted to exchange a special control protocol; the method comprising the steps of

receiving (A12; B1) a message including an address to be translated within the payload of the message by the network control device,

sending (A13; B12) a command of a special control protocol from the network control device to the network address translation device,

translating the address received by the command of the special control protocol in the network address translating device, and binding these two addresses in the network translation device for the time of the multimedia session,

sending (A14; B13) a command of the special control protocol including the translated address to the network control device.

12. The method according to claim 11, wherein the special control protocol is the MEGACO protocol.

13. The method according to claim 11, wherein the data packets including addresses within their payloads are part of Session Initiation Protocol (SIP) messages.

14. The method according to claim 11, wherein the network control device is a Call State Control Function (CSCF).

15. The method according to claim 11, wherein the network control device is a proxy.

16. The method according to claim 11, wherein the network address translation device is a Network Address Translator (NAT).

17. The method according to claim 11, wherein the network address and protocol translation device is a Network Address Translator and Protocol Translator (NAT-PT).

18. The method according to claim 11, wherein the messages exchanged are used for initiating a multimedia communication.

19. The method according to claim 18, further comprising the step of performing a dynamic binding for media addresses which are exchanged in the initiation and modification of the multimedia communication in the network address translating device (NAT or NAT-PT).

20. The method according to claim 11, further comprising a Domain Name System Application Layer Gateway (DNS-ALG) function for translating domain names to network addresses when traversing the border between the first network and the second network.

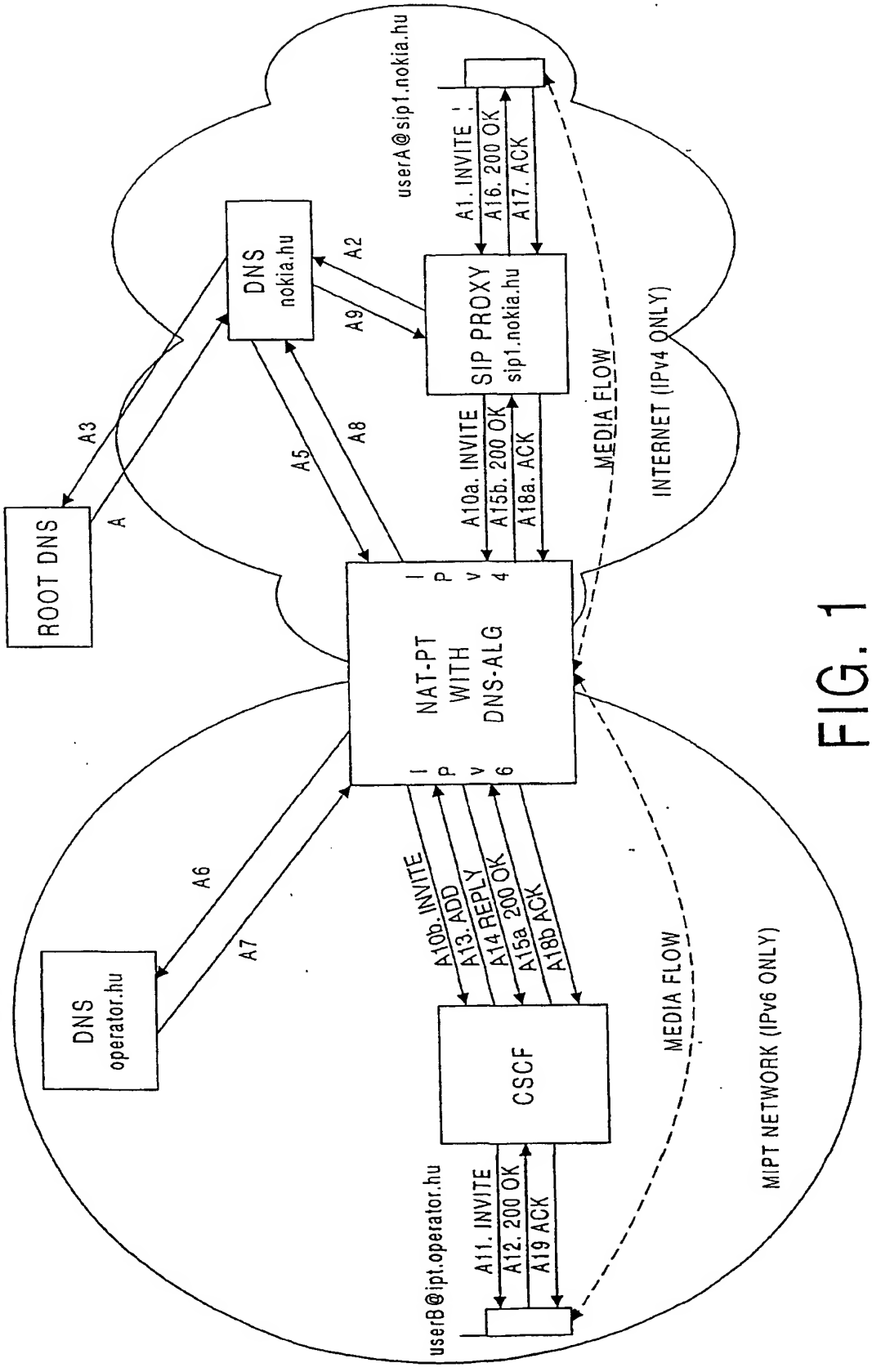

userA@sip1.nokia.hu
A1. INVITE
A16. 200 OK
A17. ACK
DNS
nokia.hu
A2
A9
SIP PROXY
sip1.nokia.hu
A3
A5
A8
A10a. INVITE
A15b. 200 OK
A18a. ACK
MEDIA FLOW
INTERNET (IPv4 ONLY)
ROOT DNS
A
NAT-PT
WITH
DNS-ALG
IPv4
IPv6
A6
A7
DNS
operator.hu
A10b. INVITE
A13. ADD
A14 REPLY
A15a 200 OK
A18b ACK
CSCF
MEDIA FLOW
MIPT NETWORK (IPv6 ONLY)
userB@ipt.operator.hu
A11. INVITE
A12. 200 OK
A19 ACK

FIG. 1

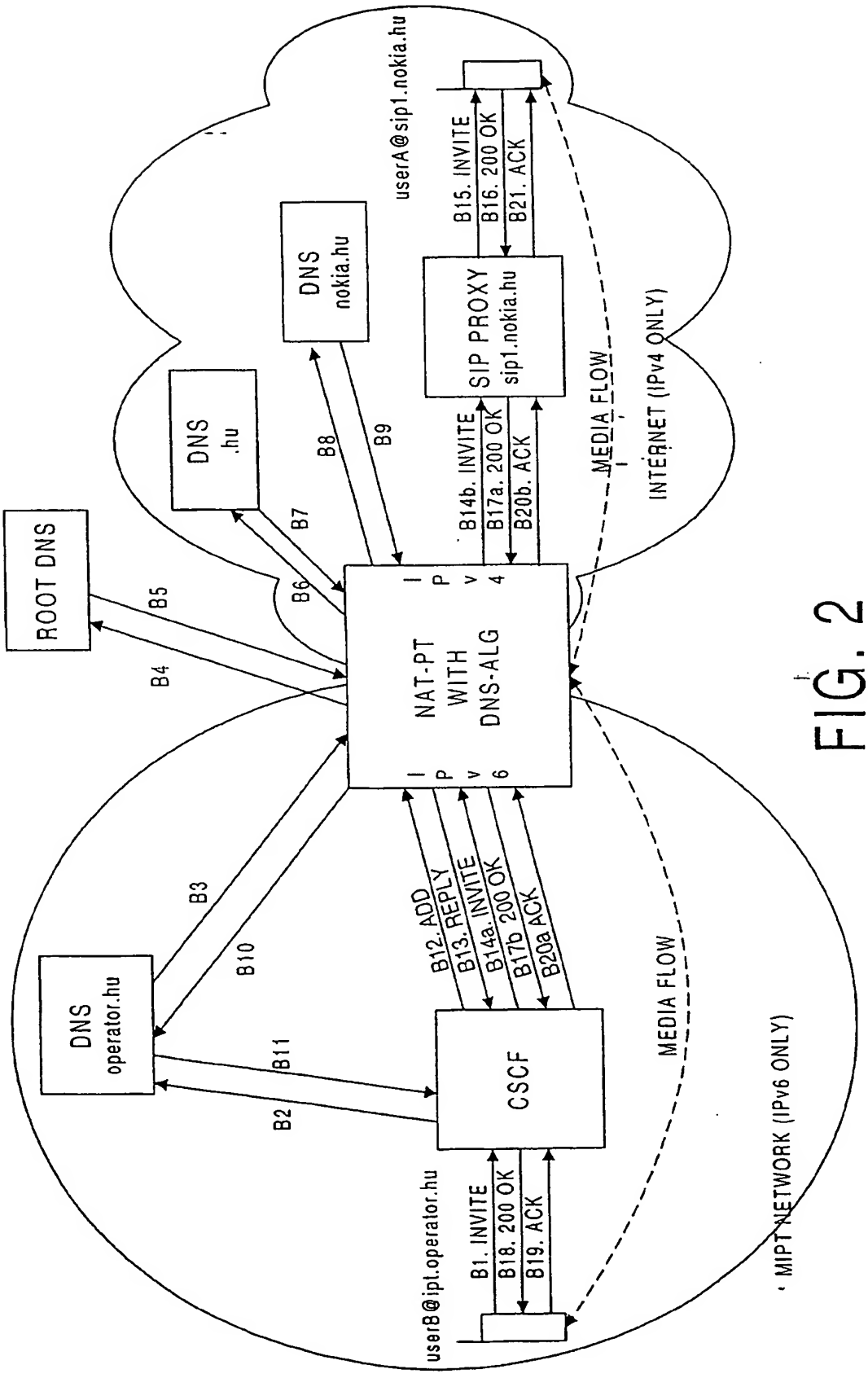

userA@sip1.nokia.hu
DNS nokia.hu
DNS .hu
ROOT DNS
SIP PROXY sip1.nokia.hu
B15. INVITE
B16. 200 OK
B21. ACK
B8
B9
B7
B6
B5
B4
B14b. INVITE
B17a. 200 OK
B20b. ACK
MEDIA FLOW
INTERNET (IPv4 ONLY)
NAT-PT WITH DNS-ALG
IPv4
IPv6
B3
B10
B12. ADD
B13. REPLY
B14a. INVITE
B17b 200 OK
B20a ACK
DNS operator.hu
B11
B2
CSCF
MEDIA FLOW
B1. INVITE
B18. 200 OK
B19. ACK
userB@ipt.operator.hu
MIPT NETWORK (IPv6 ONLY)

FIG. 2

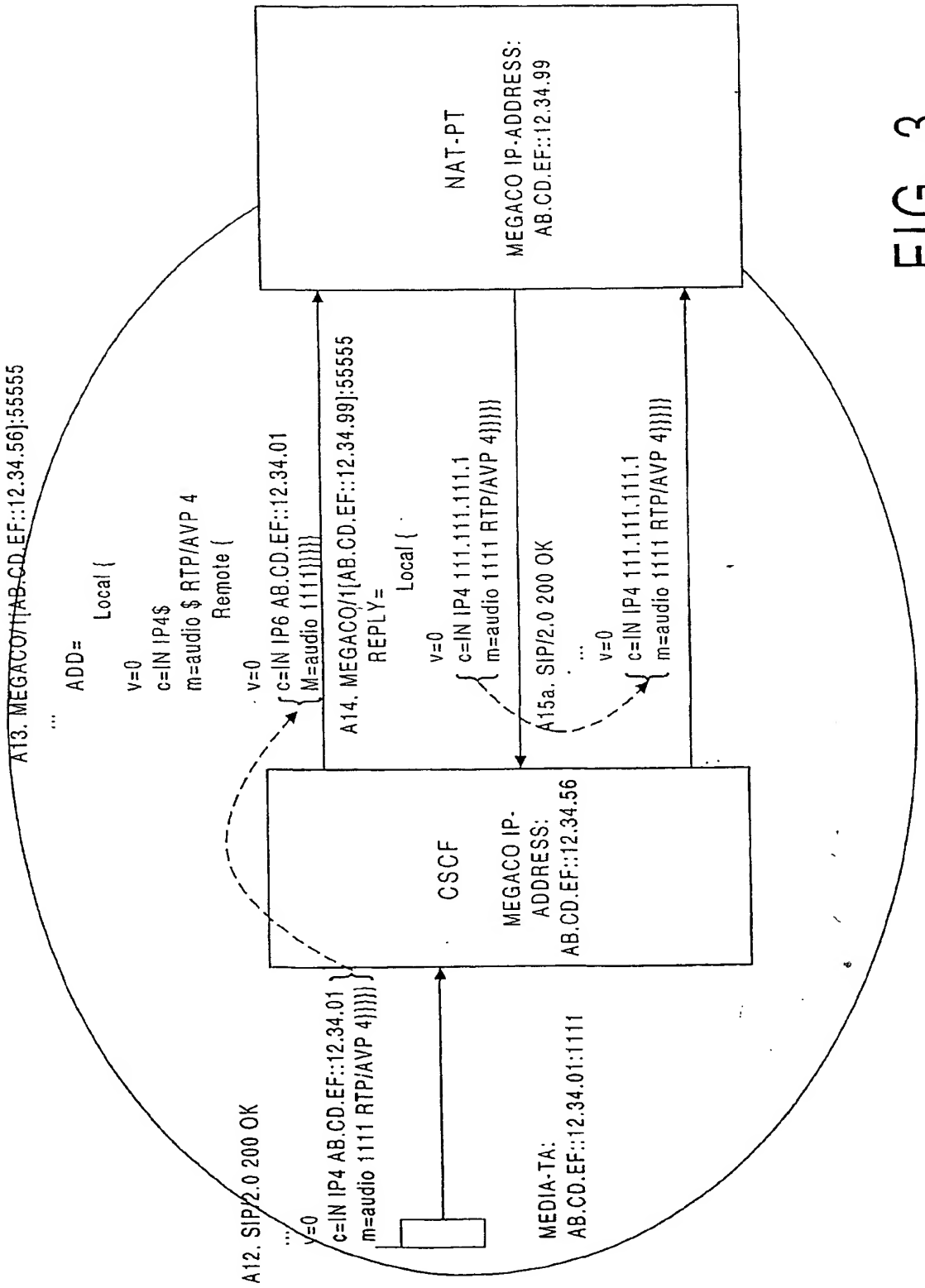

A13. MEGACO/1{AB.CD.EF::12.34.56}:55555
...
ADD=
Local {
v=0
c=IN IP4$
m=audio $ RTP/AVP 4
Remote {
v=0
c=IN IP6 AB.CD.EF::12.34.01
M=audio 1111}}}}}
A14. MEGACO/1{AB.CD.EF::12.34.99}:55555
REPLY=
Local {
v=0
c=IN IP4 111.111.111.1
m=audio 1111 RTP/AVP 4}}}}}
A15a. SIP/2.0 200 OK
...
v=0
c=IN IP4 111.111.111.1
m=audio 1111 RTP/AVP 4}}}}}
A12. SIP/2.0 200 OK
...
v=0
c=IN IP4 AB.CD.EF::12.34.01
m=audio 1111 RTP/AVP 4}}}}}
MEDIA-TA:
AB.CD.EF::12.34.01:1111
CSCF
MEGACO IP-ADDRESS:
AB.CD.EF::12.34.56
NAT-PT
MEGACO IP-ADDRESS:
AB.CD.EF::12.34.99

FIG. 3

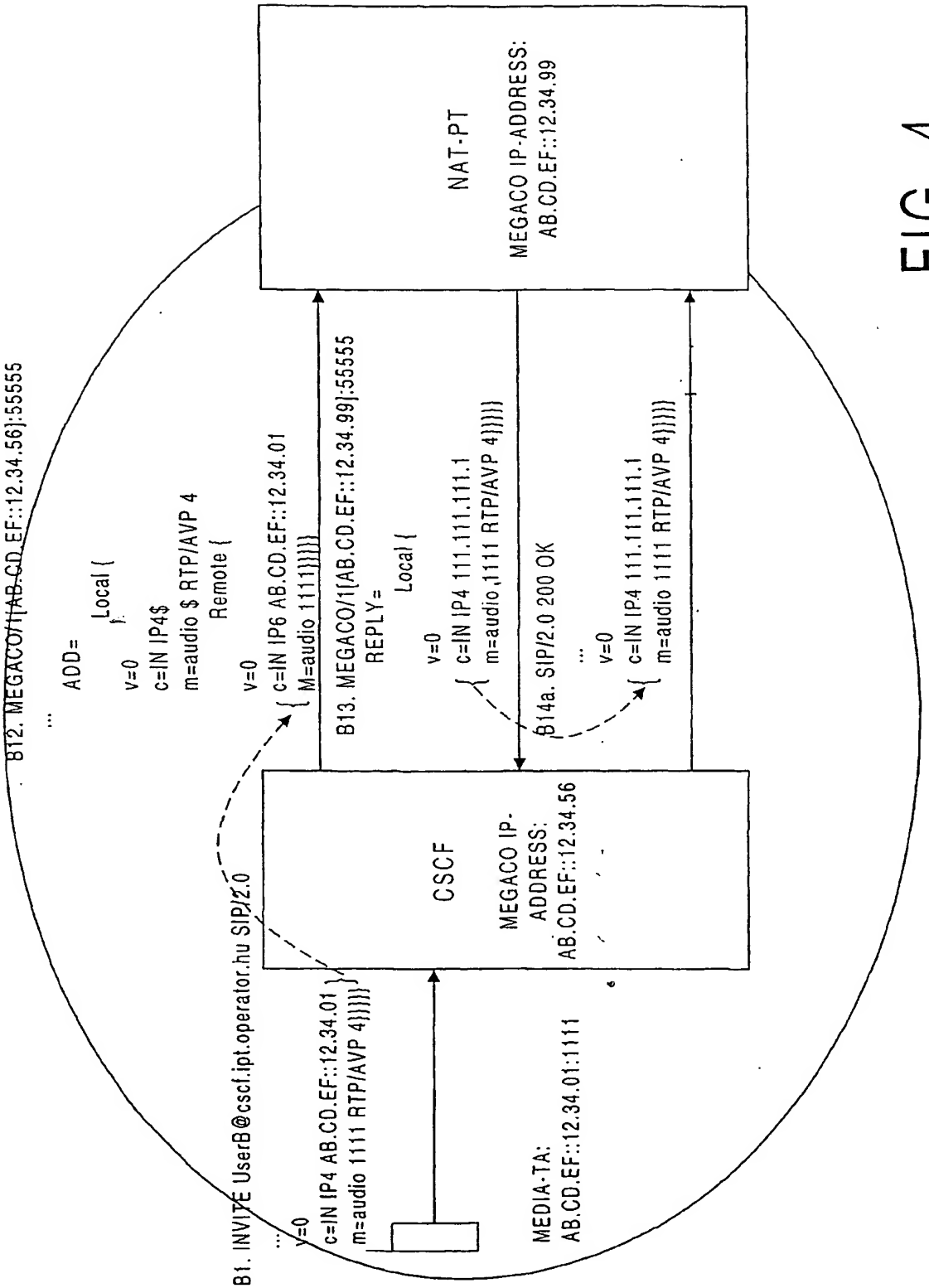

NAT-PT
MEGACO IP-ADDRESS:
AB.CD.EF::12.34.99
CSCF
MEGACO IP-
ADDRESS:
AB.CD.EF::12.34.56
MEDIA-TA:
AB.CD.EF::12.34.01:1111
B1. INVITE UserB@cscf.ipt.operator.hu SIP/2.0
...
v=0
c=IN IP4 AB.CD.EF::12.34.01
m=audio 1111 RTP/AVP 4}}}}}
B12. MEGACO/1{AB.CD.EF::12.34.56}:55555
...
ADD=
Local {
v=0
c=IN IP4$
m=audio $ RTP/AVP 4
Remote {
v=0
c=IN IP6 AB.CD.EF::12.34.01
M=audio 1111}}}}}
B13. MEGACO/1{AB.CD.EF::12.34.99}:55555
REPLY=
Local {
v=0
c=IN IP4 111.111.111.1
m=audio 1111 RTP/AVP 4}}}}}
B14a. SIP/2.0 200 OK
...
v=0
c=IN IP4 111.111.111.1
m=audio 1111 RTP/AVP 4}}}}}

FIG. 4

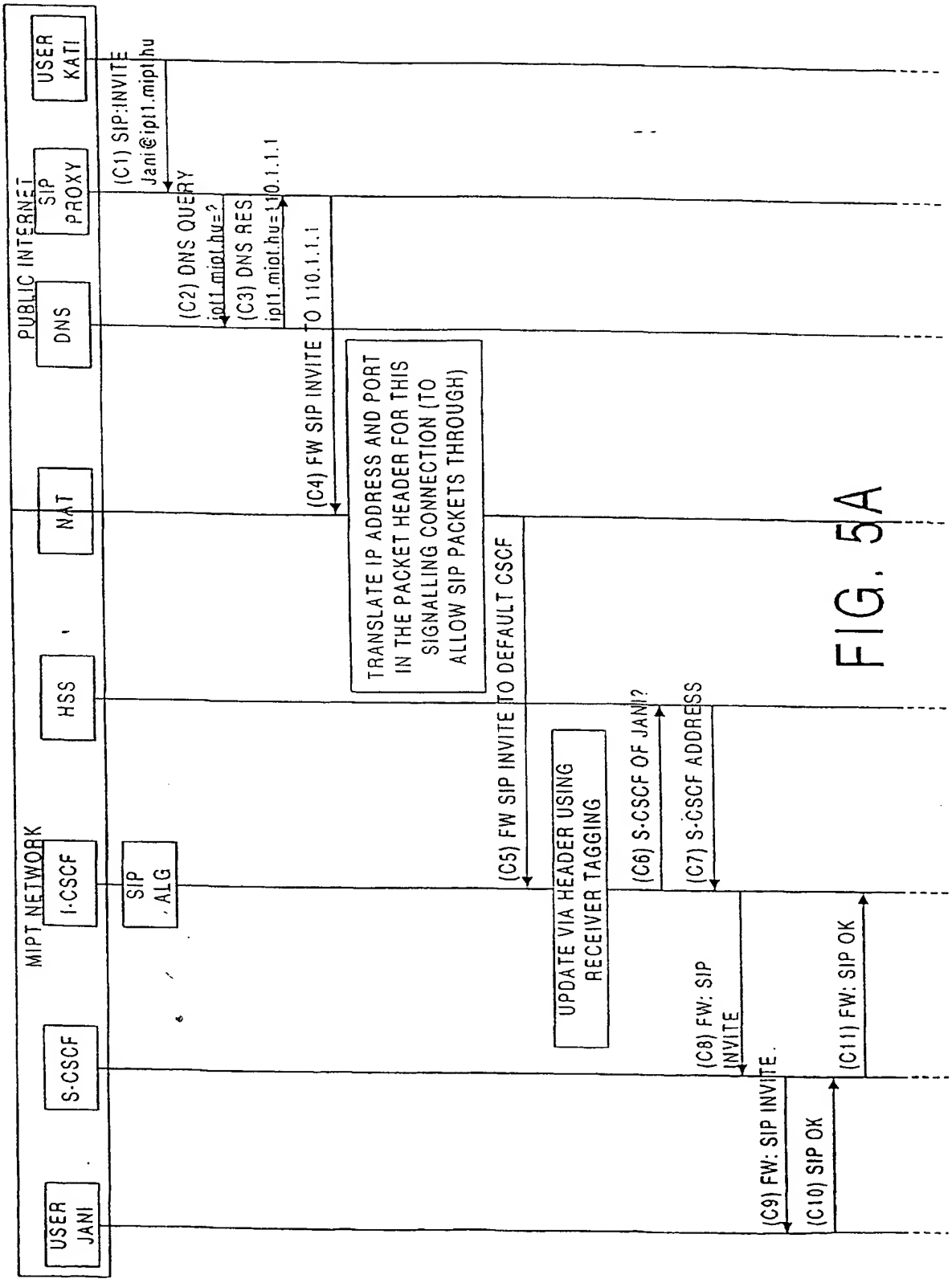

MIPT NETWORK
PUBLIC INTERNET
USER JANI
S-CSCF
I-CSCF
SIP ALG
HSS
NAT
DNS
SIP PROXY
USER KATI
(C1) SIP:INVITE Jani@ipt1.mipt.hu
(C2) DNS QUERY ipt1.miot.hu=?
(C3) DNS RES ipt1.miot.hu=110.1.1.1
(C4) FW SIP INVITE TO 110.1.1.1
TRANSLATE IP ADDRESS AND PORT IN THE PACKET HEADER FOR THIS SIGNALLING CONNECTION (TO ALLOW SIP PACKETS THROUGH)
(C5) FW SIP INVITE TO DEFAULT CSCF
UPDATE VIA HEADER USING RECEIVER TAGGING
(C6) S-CSCF OF JANI?
(C7) S-CSCF ADDRESS
(C8) FW: SIP INVITE
(C9) FW: SIP INVITE
(C10) SIP OK
(C11) FW: SIP OK

FIG. 5A

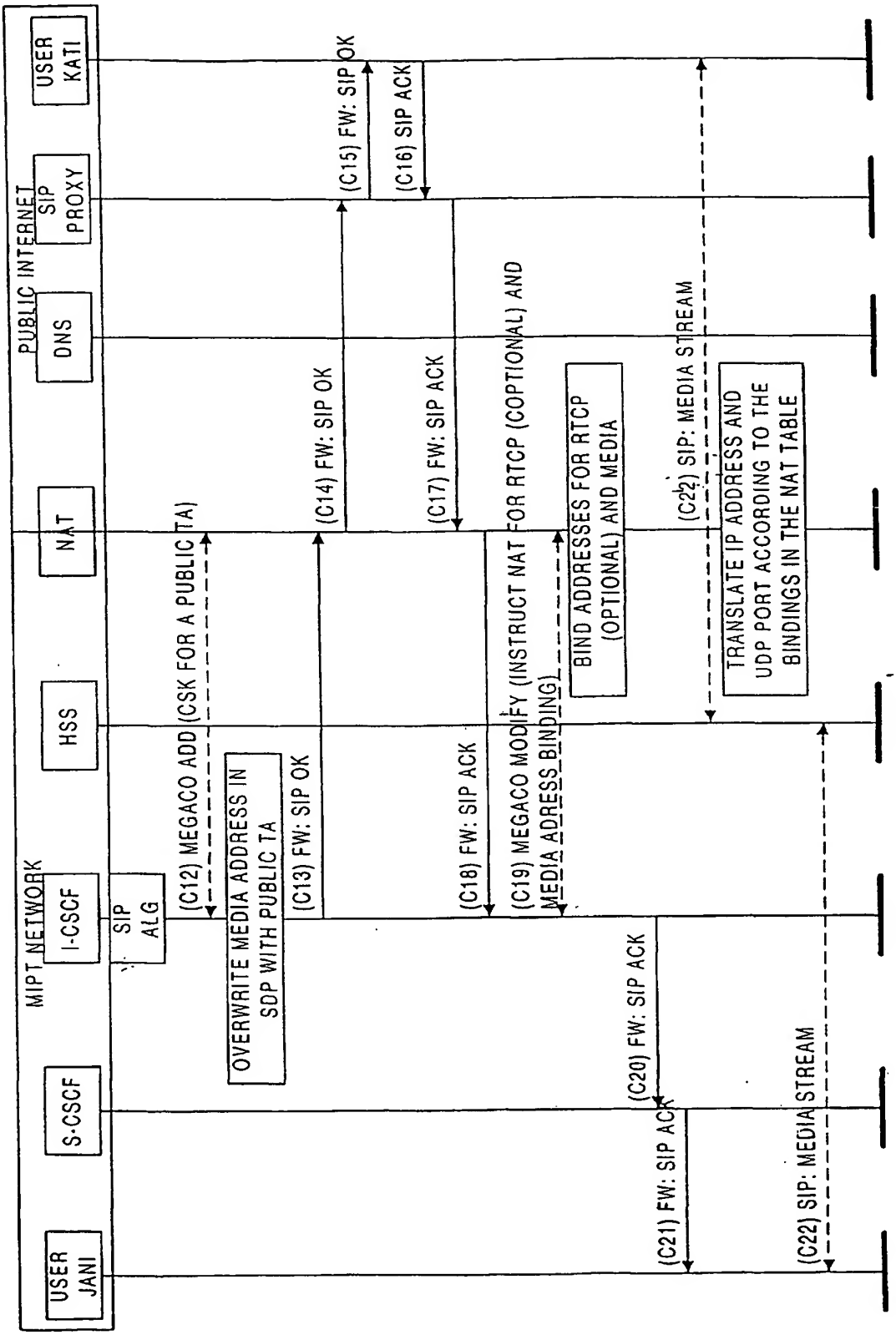

MIPT NETWORK
PUBLIC INTERNET
USER JANI
S-CSCF
I-CSCF
SIP ALG
HSS
NAT
DNS
SIP PROXY
USER KATI
(C12) MEGACO ADD (CSK FOR A PUBLIC TA)
OVERWRITE MEDIA ADDRESS IN SDP WITH PUBLIC TA
(C13) FW: SIP OK
(C14) FW: SIP OK
(C15) FW: SIP OK
(C16) SIP ACK
(C17) FW: SIP ACK
(C18) FW: SIP ACK
(C19) MEGACO MODIFY (INSTRUCT NAT FOR RTCP (COPTIONAL) AND MEDIA ADRESS BINDING)
BIND ADDRESSES FOR RTCP (OPTIONAL) AND MEDIA
(C20) FW: SIP ACK
(C21) FW: SIP ACK
(C22) SIP: MEDIA STREAM
(C22) SIP: MEDIA STREAM
TRANSLATE IP ADDRESS AND UDP PORT ACCORDING TO THE BINDINGS IN THE NAT TABLE

FIG. 5B

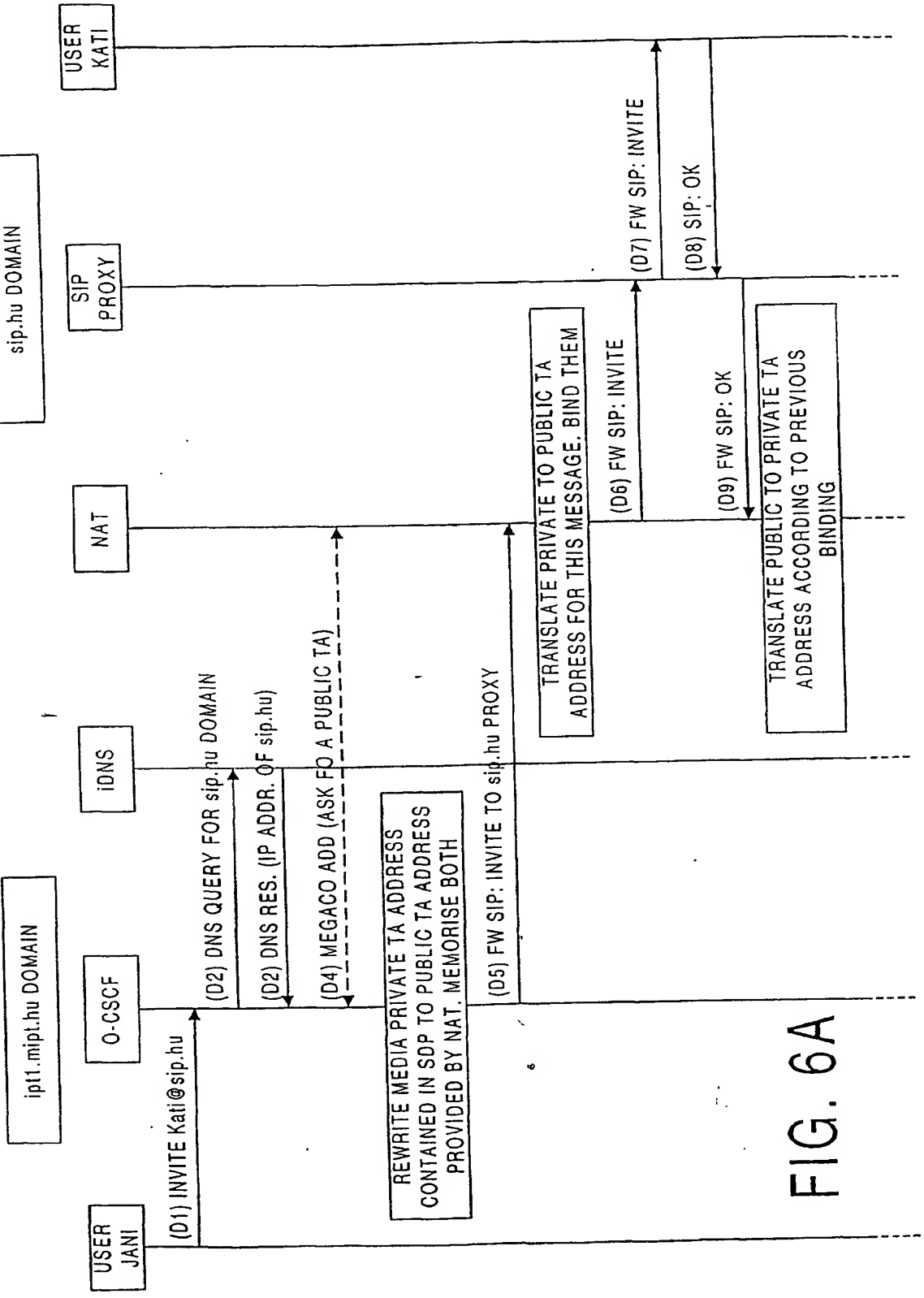

USER JANI
ipt1.mipt.hu DOMAIN
O-CSCF
iDNS
NAT
sip.hu DOMAIN
SIP PROXY
USER KATI
(D1) INVITE Kati@sip.hu
(D2) DNS QUERY FOR sip.hu DOMAIN
(D2) DNS RES. (IP ADDR. OF sip.hu)
(D4) MEGACO ADD (ASK FO A PUBLIC TA)
REWRITE MEDIA PRIVATE TA ADDRESS CONTAINED IN SDP TO PUBLIC TA ADDRESS PROVIDED BY NAT. MEMORISE BOTH
(D5) FW SIP: INVITE TO sip.hu PROXY
TRANSLATE PRIVATE TO PUBLIC TA ADDRESS FOR THIS MESSAGE. BIND THEM
(D6) FW SIP: INVITE
(D7) FW SIP: INVITE
(D8) SIP: OK
(D9) FW SIP: OK
TRANSLATE PUBLIC TO PRIVATE TA ADDRESS ACCORDING TO PREVIOUS BINDING

FIG. 6A

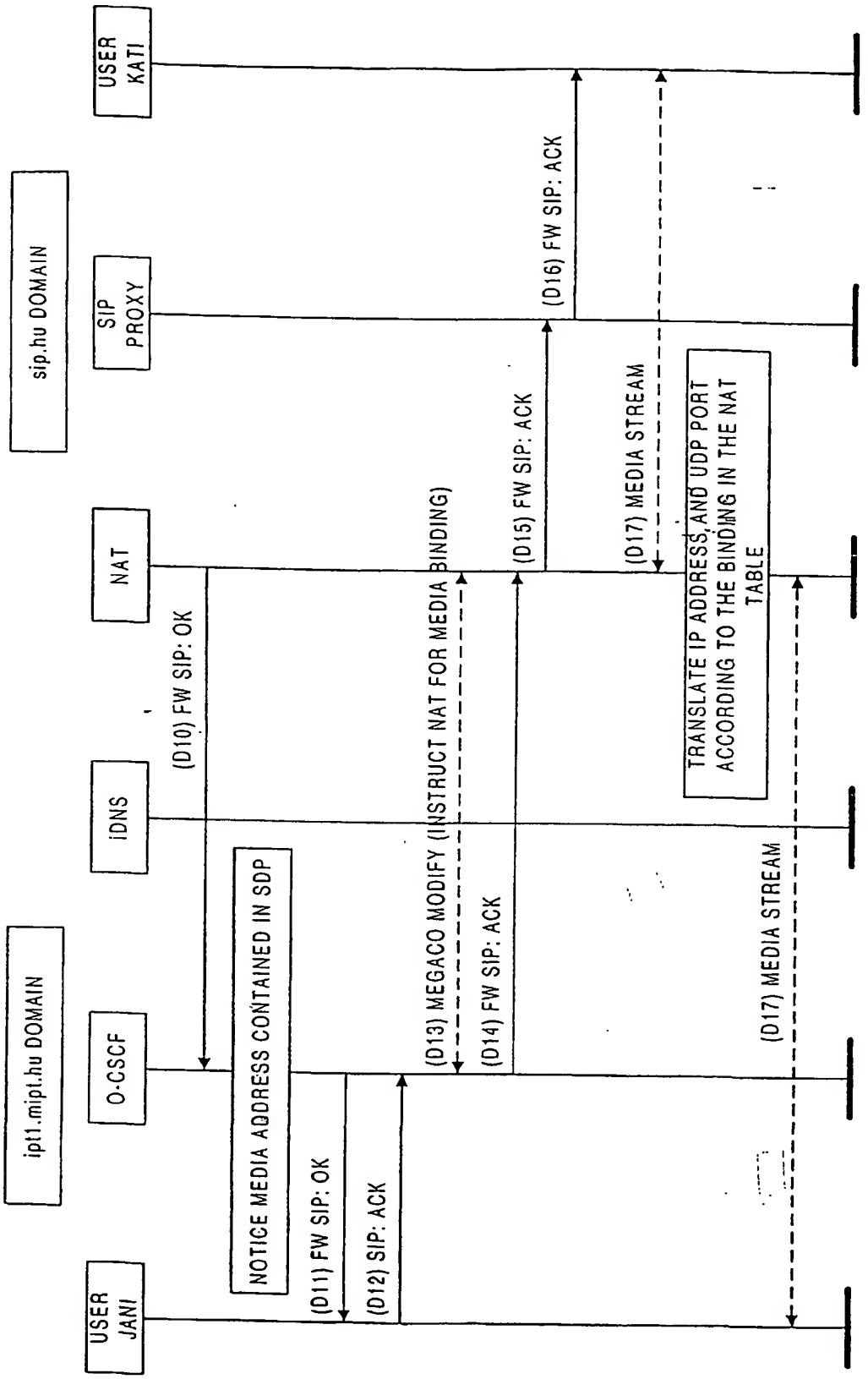

USER KATI
sip.hu DOMAIN
SIP PROXY
NAT
iDNS
ipt1.mipt.hu DOMAIN
O-CSCF
USER JANI
(D10) FW SIP: OK
NOTICE MEDIA ADDRESS CONTAINED IN SDP
(D11) FW SIP: OK
(D12) SIP: ACK
(D13) MEGACO MODIFY (INSTRUCT NAT FOR MEDIA BINDING)
(D14) FW SIP: ACK
(D15) FW SIP: ACK
(D16) FW SIP: ACK
(D17) MEDIA STREAM
TRANSLATE IP ADDRESS AND UDP PORT ACCORDING TO THE BINDING IN THE NAT TABLE
(D17) MEDIA STREAM

FIG. 6B

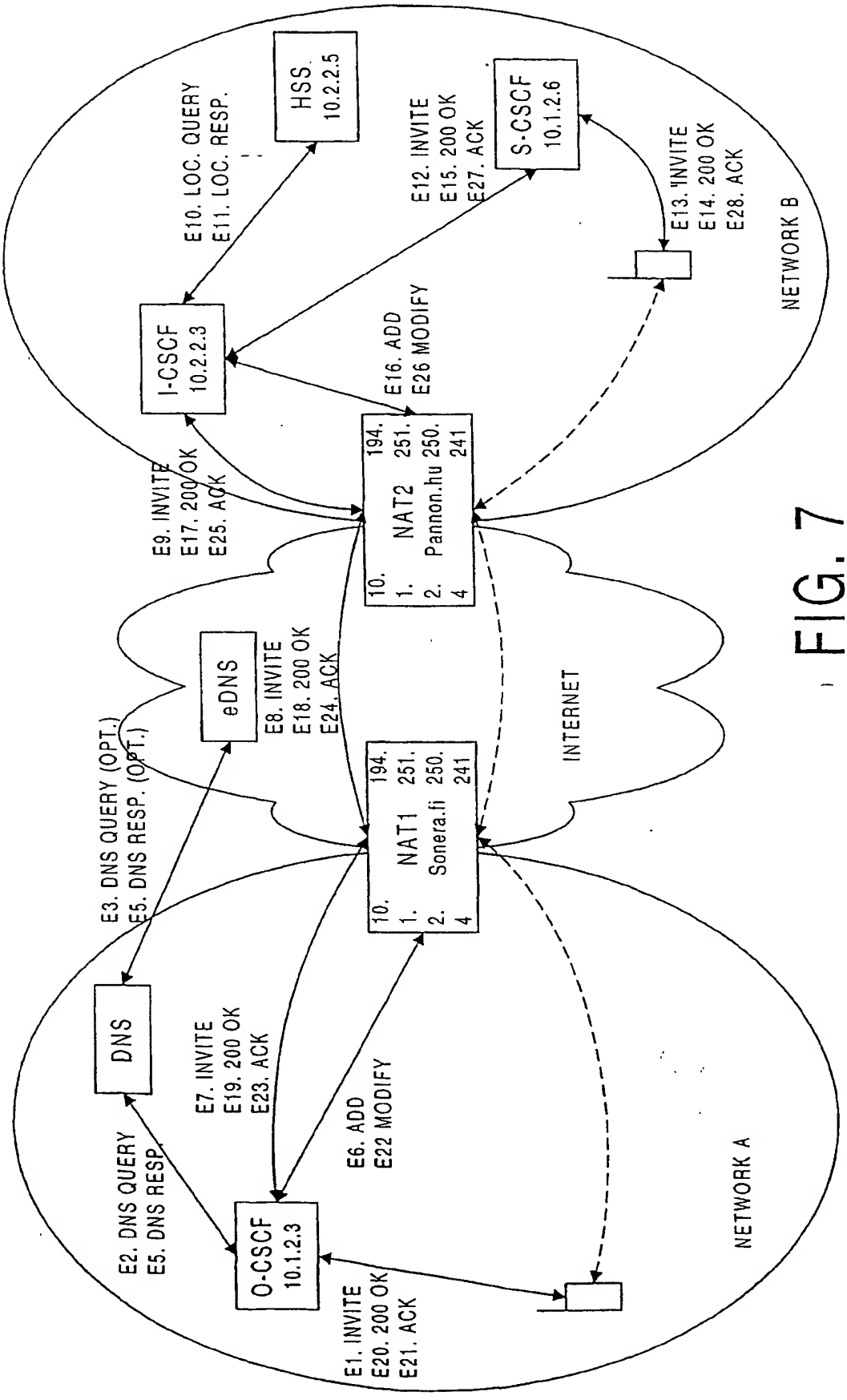

NETWORK A
NETWORK B
INTERNET
O-CSCF
10.1.2.3
I-CSCF
10.2.2.3
S-CSCF
10.1.2.6
HSS
10.2.2.5
DNS
eDNS
NAT1
10.
1.
2.
4
194.
251.
250.
241
Sonera.fi
NAT2
Pannon.hu
E1. INVITE
E20. 200 OK
E21. ACK
E2. DNS QUERY
E5. DNS RESP.
E3. DNS QUERY (OPT.)
E5. DNS RESP. (OPT.)
E6. ADD
E22 MODIFY
E7. INVITE
E19. 200 OK
E23. ACK
E8. INVITE
E18. 200 OK
E24. ACK
E9. INVITE
E17. 200 OK
E25. ACK
E10. LOC. QUERY
E11. LOC. RESP.
E12. INVITE
E15. 200 OK
E27. ACK
E13. INVITE
E14. 200 OK
E28. ACK
E16. ADD
E26 MODIFY

FIG. 7

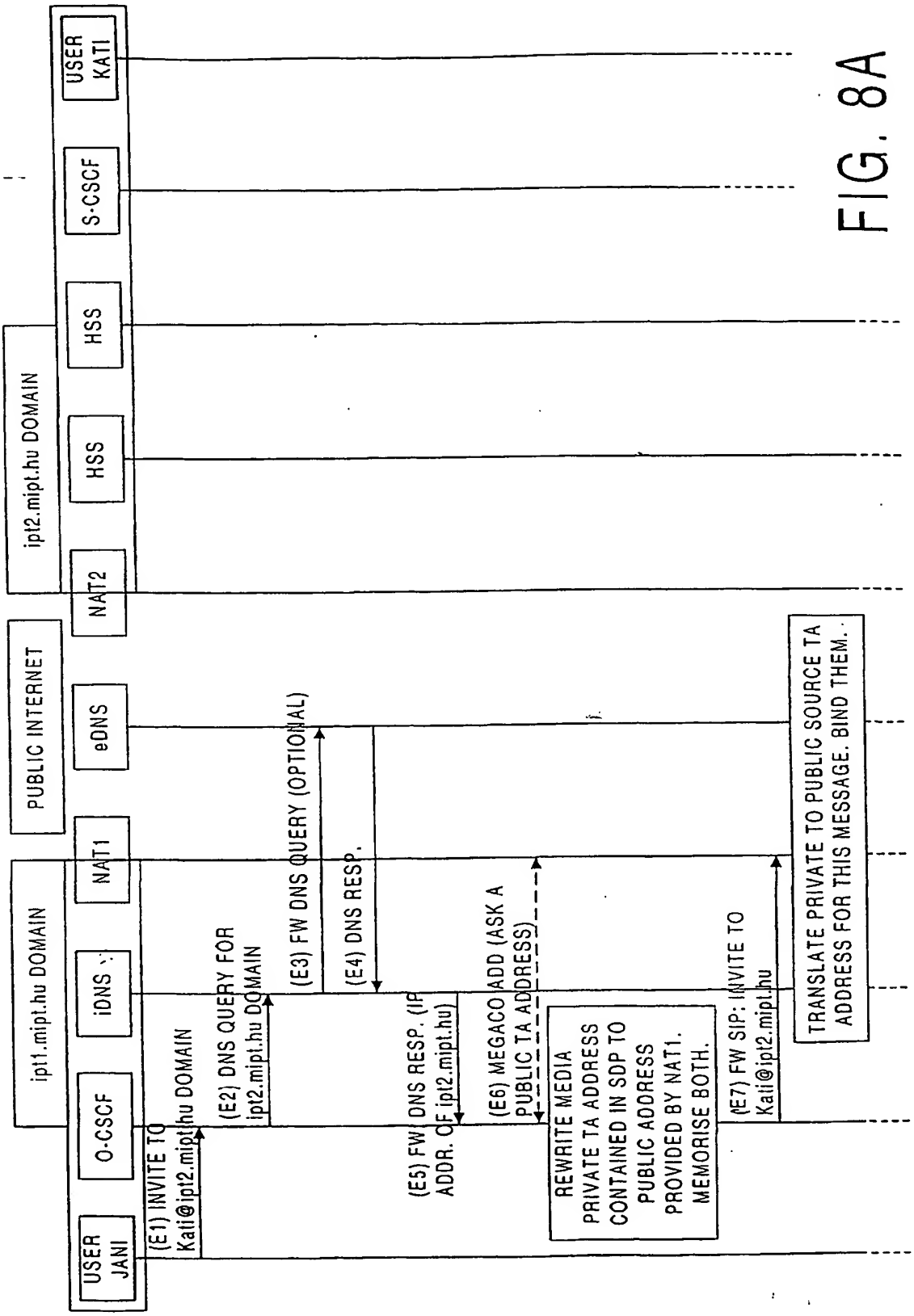

USER JANI
O-CSCF
iDNS
NAT1
eDNS
NAT2
HSS
HSS
S-CSCF
USER KATI
ipt1.mipt.hu DOMAIN
PUBLIC INTERNET
ipt2.mipt.hu DOMAIN
(E1) INVITE TO Kati@ipt2.mipt.hu DOMAIN
(E2) DNS QUERY FOR ipt2.mipt.hu DOMAIN
(E3) FW DNS QUERY (OPTIONAL)
(E4) DNS RESP.
(E5) FW DNS RESP. (IP ADDR. OF ipt2.mipt.hu)
(E6) MEGACO ADD (ASK A PUBLIC TA ADDRESS)
REWRITE MEDIA PRIVATE TA ADDRESS CONTAINED IN SDP TO PUBLIC ADDRESS PROVIDED BY NAT1. MEMORISE BOTH.
(E7) FW SIP: INVITE TO Kati@ipt2.mipt.hu
TRANSLATE PRIVATE TO PUBLIC SOURCE TA ADDRESS FOR THIS MESSAGE. BIND THEM.

FIG. 8A

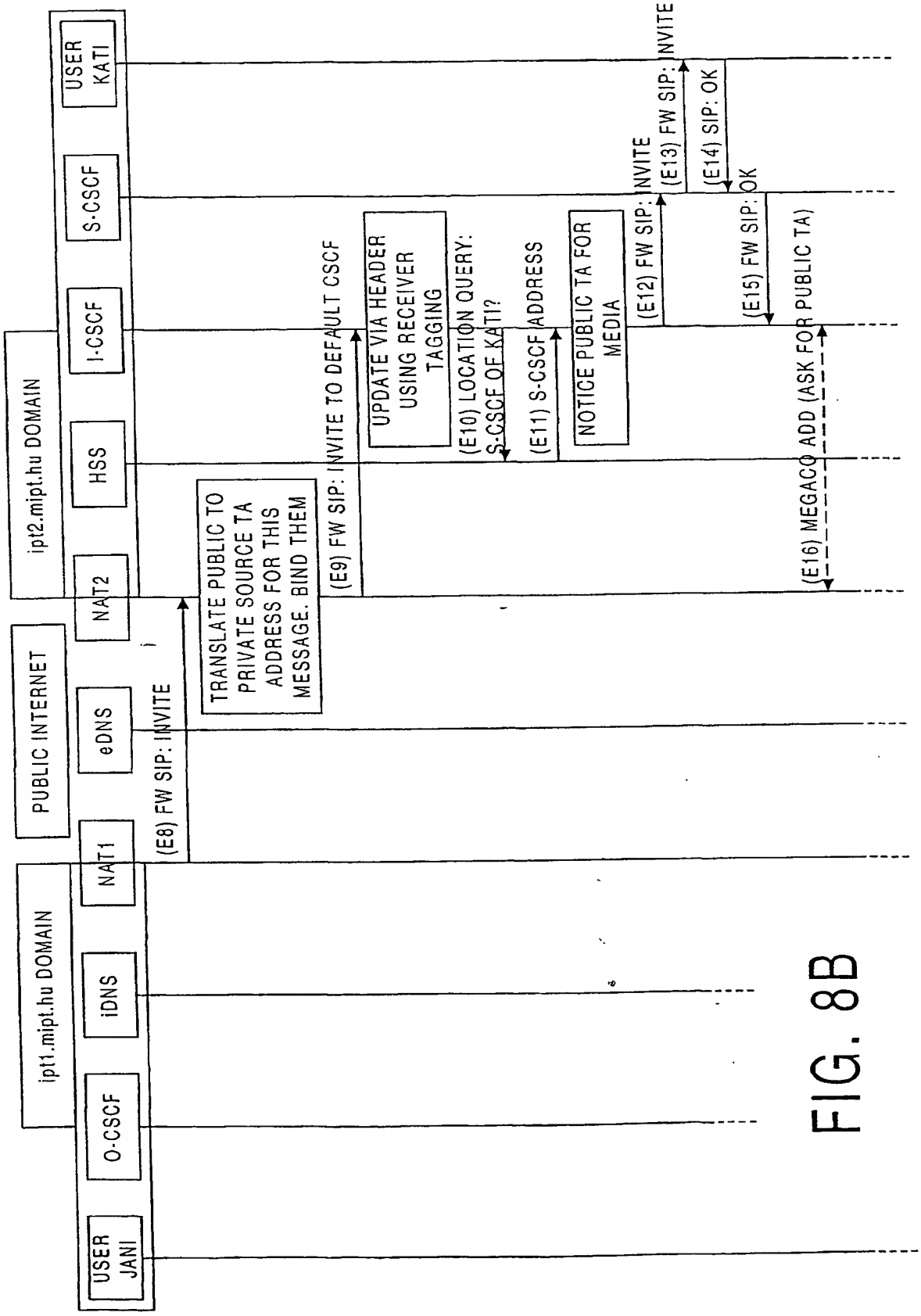

ipt1.mipt.hu DOMAIN
USER JANI
O-CSCF
iDNS
NAT1
PUBLIC INTERNET
eDNS
NAT2
ipt2.mipt.hu DOMAIN
HSS
I-CSCF
S-CSCF
USER KATI
(E8) FW SIP: INVITE
TRANSLATE PUBLIC TO PRIVATE SOURCE TA ADDRESS FOR THIS MESSAGE. BIND THEM
(E9) FW SIP: INVITE TO DEFAULT CSCF
UPDATE VIA HEADER USING RECEIVER TAGGING
(E10) LOCATION QUERY: S-CSCF OF KATI?
(E11) S-CSCF ADDRESS
NOTICE PUBLIC TA FOR MEDIA
(E12) FW SIP: INVITE
(E13) FW SIP: INVITE
(E14) SIP: OK
(E15) FW SIP: OK
(E16) MEGACO ADD (ASK FOR PUBLIC TA)

FIG. 8B

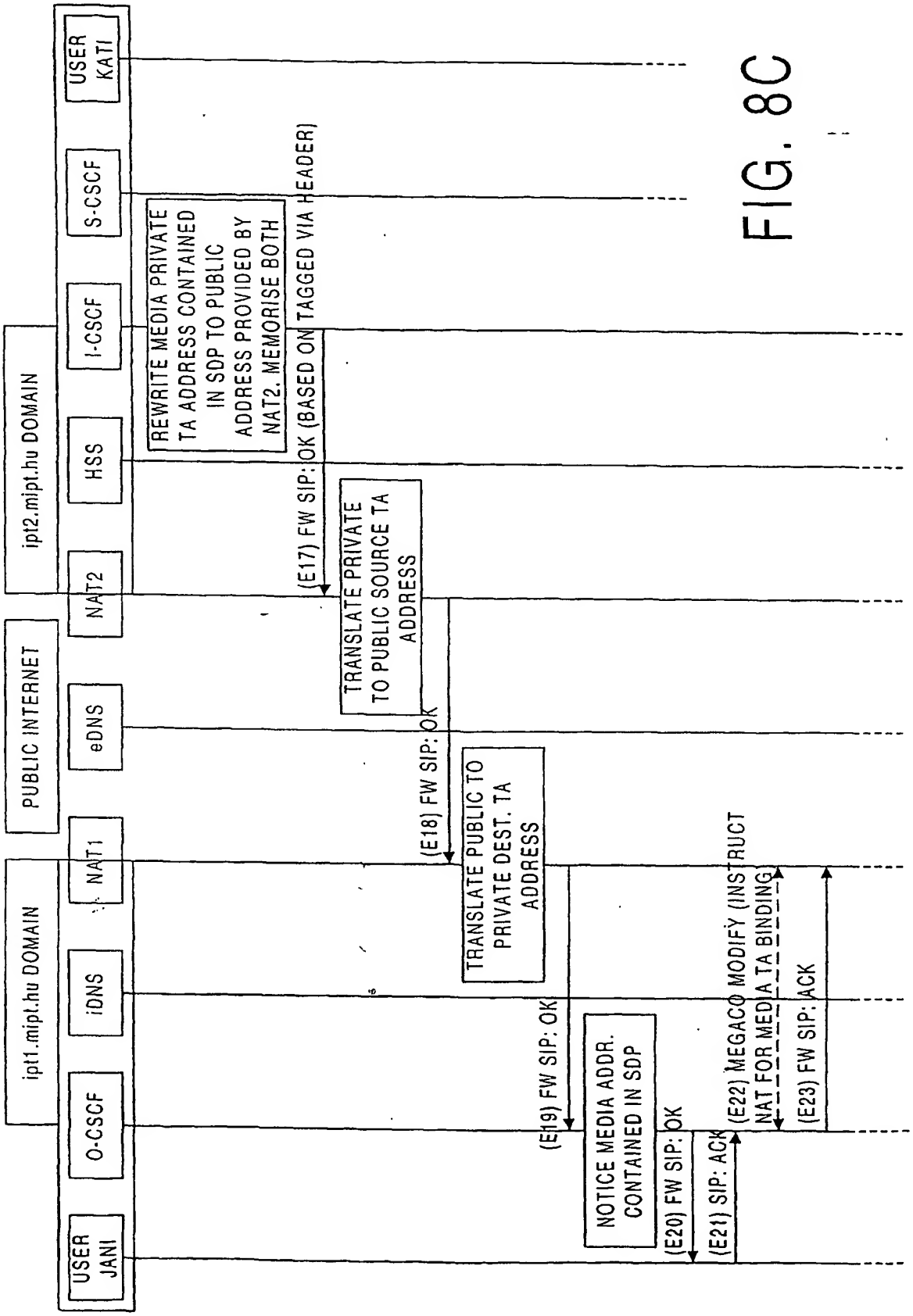
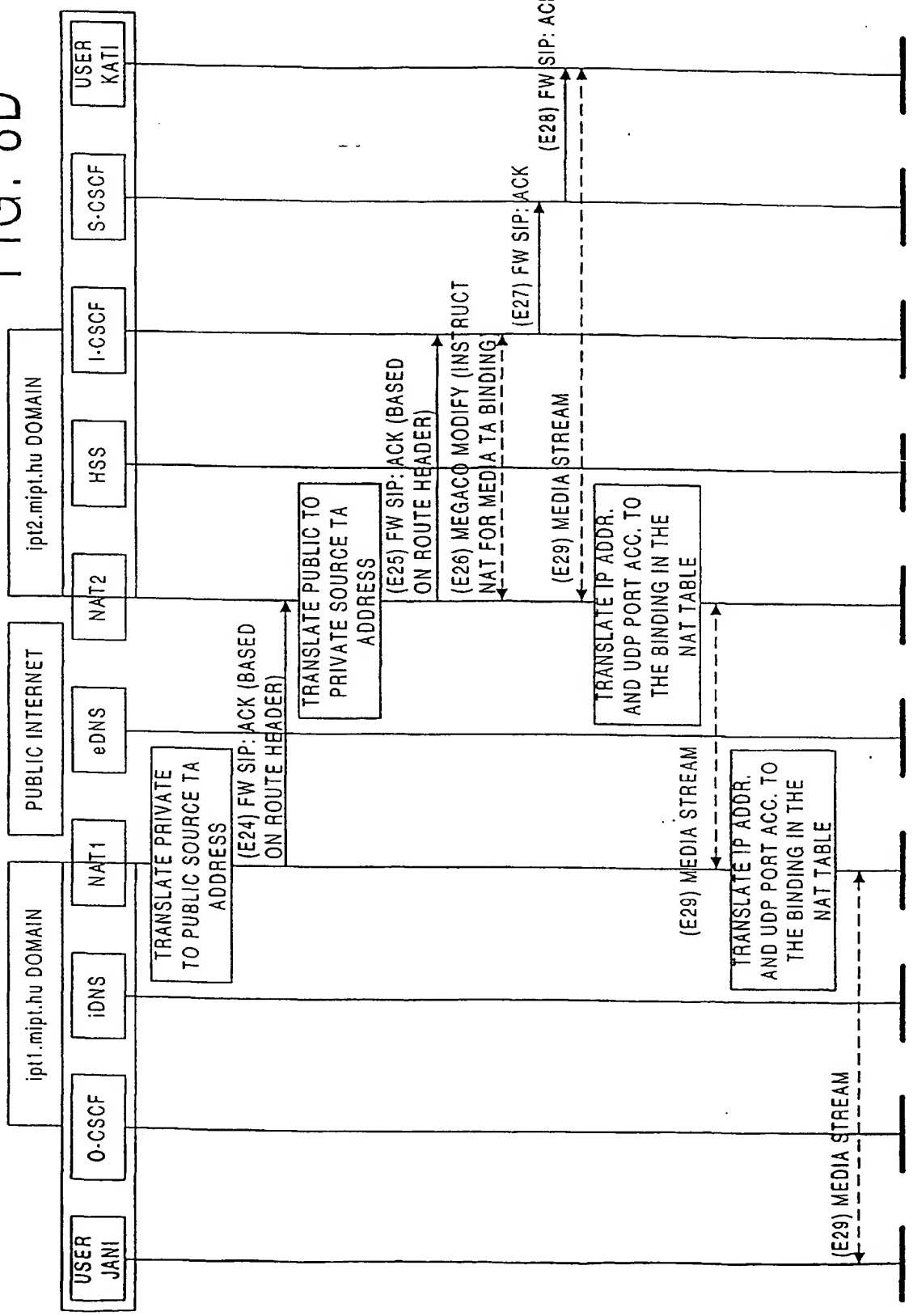

USER JANI
ipt1.mipt.hu DOMAIN
O-CSCF
iDNS
NAT1
PUBLIC INTERNET
eDNS
NAT2
ipt2.mipt.hu DOMAIN
HSS
I-CSCF
S-CSCF
USER KATI
REWRITE MEDIA PRIVATE TA ADDRESS CONTAINED IN SDP TO PUBLIC ADDRESS PROVIDED BY NAT2. MEMORISE BOTH
(E17) FW SIP: OK (BASED ON TAGGED VIA HEADER)
TRANSLATE PRIVATE TO PUBLIC SOURCE TA ADDRESS
(E18) FW SIP: OK
TRANSLATE PUBLIC TO PRIVATE DEST. TA ADDRESS
(E19) FW SIP: OK
NOTICE MEDIA ADDR. CONTAINED IN SDP
(E20) FW SIP: OK
(E21) SIP: ACK
(E22) MEGACO MODIFY (INSTRUCT NAT FOR MEDIA TA BINDING
(E23) FW SIP: ACK

FIG. 8C

FIG. 8D


USER JANI
O-CSCF
iDNS
NAT1
ipt1.mipt.hu DOMAIN
PUBLIC INTERNET
eDNS
NAT2
ipt2.mipt.hu DOMAIN
HSS
I-CSCF
S-CSCF
USER KATI
TRANSLATE PRIVATE TO PUBLIC SOURCE TA ADDRESS
(E24) FW SIP: ACK (BASED ON ROUTE HEADER)
TRANSLATE PUBLIC TO PRIVATE SOURCE TA ADDRESS
(E25) FW SIP: ACK (BASED ON ROUTE HEADER)
(E26) MEGACO MODIFY (INSTRUCT NAT FOR MEDIA TA BINDING)
(E27) FW SIP: ACK
(E28) FW SIP: ACK
(E29) MEDIA STREAM
TRANSLATE IP ADDR. AND UDP PORT ACC. TO THE BINDING IN THE NAT TABLE
(E29) MEDIA STREAM
TRANSLATE IP ADDR. AND UDP PORT ACC. TO THE BINDING IN THE NAT TABLE
(E29) MEDIA STREAM

INTERNATIONAL SEARCH REPORT

Interni I Application No
PCT/EP 00/07037

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06 H04L29/12

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, INSPEC, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	J. ROSENBERG, D. DREW, H. SCHULZRINNE: "Getting SIP through Firewalls and NATs" INTERNET DRAFT, 'Online! 22 February 2000 (2000-02-22), pages 1-29, XP002167710 Retrieved from the Internet: <URL:http://www.softarmor.com/sipwg/draft-rosenberg-sip-firewalls-00.txt> 'retrieved on 2001-05-18!	1,3, 5-11,13, 15-20
Y	abstract paragraph '0001! paragraph '02.2! - paragraph '06.5! paragraph '6.10!	2,4,12, 14

-/--

[X] Further documents are listed in the continuation of box C. [ ] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
25 May 2001	07/06/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Lievens, K

Form PCT/ISA/210 (second sheet) (July 1992)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	A. NAPOLITANO, G. RICAGNI: "UMTS all-IP Mobility Management, Call and Session Control Procedures" INTERNET DRATFT, 'Online! 24 March 2000 (2000-03-24), pages 1-17, XP002149519 Retrieved from the Internet: <URL:http://www.alternic.org/drafts/draft-ricagni-megaco-umts-all-ip-00.txt> 'retrieved on 2001-05-18! paragraph '0001! - paragraph '0004!	2,4,12, 14
A	G. TSIRTSIS, P. SRISURESH: "RFC2766: Network Address Translation - Protocol Translation (NAT-PT)" REQUEST FOR COMMENT, 'Online! February 2000 (2000-02), pages 1-15, XP002167711 Retrieved from the Internet: <URL:http://www.faqs.org/rfcs/rfc2766.html > 'retrieved on 2001-05-18! abstract paragraph '0001! - paragraph '0006!	6,19